NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

METRIC METHODOLOGY FOR THE CREATION OF ENVIRONMENTS AND PROCESSES TO CERTIFY A COMPONENT: THE NRL PUMP

by

Jonathan S. Holmgren Sr.
Ronald P. Rich

March 2003

Thesis Advisor: George Dinolt
Co-Advisor: Craig Rasmussen

This thesis was completed in cooperation with the Cebrowski Institute for Information Innovation and Superiority.

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Metric Methodology for the Creation of Environments and Processes to Certify a Component: the NRL Pump			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jonathan S. Holmgren Sr. and Ronald P. Rich			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** UL

13. ABSTRACT ***(maximum 200 words)***

Information superiority has many components. Of critical importance is information security. Over forty years ago when information security for computer based systems started being discussed, the military leadership looked for general purpose, high-assurance, multi-level secure (MLS) computers and software. Information is compiled at various data sensitivity levels, but it also incorporates low-level data with high-level data to provide the necessary information at the system high-level being evaluated. What is the best way to get the low-level data to the high-level system/user without compromising the high-level system?

One proposed solution is the Naval Research Laboratory's (NRL) Network Pump (NP) to prevent unauthorized information flow between computers of different security levels. To incorporate the NP into the DoD infrastructure it is necessary to get the NP through the hurdle of Certification and Accreditation. The NRL has produced and provided many useful documents for the C&A of the NP, but the key requirement for Certification and Accreditation is the creation of a Protection Profile and an understanding of the DITSCAP requirements and process. This thesis creates a Protection Profile for the NP along with a draft Type SSAA for Certification and Accreditation of the NP.

14. SUBJECT TERMS NRL Pump, Protection Profile, DITSCAP, Common Criteria, Trusted Guard, EAL5, Type SSAA, Certification and Accreditation, Multi-level Security (MLS), Information Assurance, Network Pump, Data Pump, Covert Channels, and High Assurance Component.			**15. NUMBER OF PAGES** 175
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited
This thesis was completed in cooperation with the Cebrowski Institute for Information Innovation and Superiority.

METRIC METHODOLOGY FOR THE CREATION OF ENVIRONMENTS AND PROCESSES TO CERTIFY A COMPONENT; SPECIFICALLY THE NAVAL RESEARCH LABORATORY PUMP

Jonathan S. Holmgren Sr.
Lieutenant, United States Navy
B.S., The University of Kansas, 1996

and

Ronald P. Rich
Lieutenant, United States Navy
B.S., Oregon State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2003

Authors: Jonathan S. Holmgren Sr.

Ronald P. Rich

Approved by: George Dinolt
Thesis Advisor

Craig Rasmussen
Co-Advisor

Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information superiority has many components. Of critical importance is information security. Over forty years ago, when information security for computer based systems started being discussed, the military leadership looked for general-purpose, high-assurance, multi-level secure (MLS) computers and software. Information is compiled at various data sensitivity levels, but it also incorporates low-level data with high-level data to provide the necessary information at the system high-level being evaluated. What is the best way to get the low-level data to the high-level system/user without compromising the high-level system?

One proposed solution is the Naval Research Laboratory's (NRL) Network Pump (NP) to prevent unauthorized information flow between computers of different security levels. To incorporate the NP into the DoD infrastructure it is necessary to get the NP through the hurdle of Certification and Accreditation. The NRL has produced and provided many useful documents for the C&A of the NP, but the key requirement for Certification and Accreditation is the creation of a Protection Profile and an understanding of the DITSCAP requirements and process. This thesis creates a Protection Profile for the NP along with a draft Type SSAA for Certification and Accreditation of the NP.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. NAVAL RESEARCH LABORATORY NETWORK PUMP

A. INTRODUCTION

With the advances being made in technology and the shift in the Navy and Department of Defense to Network Centric Warfare, the need for information superiority has never been more critical. Information superiority has many components. Of critical importance is information security. Over forty years ago, when information security for computer-based systems was first discussed, the military leadership looked for general purpose, high-assurance, multi-level secure (MLS) computers and software. These modes of thinking led us to the systems we have today. What we have discovered, though, is that these systems are extremely difficult to build and difficult to incorporate into an operational environment, because of their expense and user hostile operating environment. We have also discovered that, since industry does not require or support our specialized security needs, DoD was forced to create specialized systems and code. As a result these projects are difficult to scale.

Because of the learning curve the DoD has endured, we now know that part of the information security answer lies in a scalable security solution that does not depend on general-purpose MLS systems. Instead, we need to use commercial products for general-purpose computing, incorporated with special-purpose and trusted devices, for the separation of data at different security levels.

B. CURRENT WAY OF DOING BUSINESS

The military currently uses the DoD Security Clearances and Classifications of Unclassified, Confidential, Secret, Top Secret, Top Secret/Sensitive Information, and Compartmentalization (defined in Appendix B) [Ref. 1]. Its users operate at different levels, and a majority of the time at multiple levels, within the organizational structure. Information is compiled at various data sensitivity levels, but it also incorporates low-level data with high-level data to provide the necessary information at the system high-level being evaluated. This is where the problem comes in. What is the best way to get the low-level data to the high-level system/user without compromising the low-level system? The process being used today is the manual method. A user, for example, might

prepare a Top Secret Brief for the daily meeting. The required information for the brief, to be comprehensive, resides at the Unclassified, Secret and Top Secret levels. The user must go to each system, identify what data is required, save it to a disk (at each level), put the disk in the Top Secret system and consolidate the data. This data may reside in the same space, building, or in any variety of different locations. Once the disk is placed in the Top Secret system it is now classified as Top Secret and cannot be used again in a lower-level system. This is always the case when data is being transferred from a low-level system to a high-level system over an external medium. The medium gets classified to the level of the highest system it is introduced to. This process results in many man-hours, numerous disks that become classified at system high, and the need to declassify or account for new classified media. It is very easy for a user to fail to properly label the disk or inadvertently place the high-level disk in a low-level system, compromising the low-level system, creating security violations and potential information security leaks.

A solution to this problem is to provide a means to transfer information from a lower sensitivity level to a higher one efficiently and effectively over a secure medium without compromising either system. In this one can create a multi-level secure system out of COTS components and a simple communications component. One proposed solution is the Naval Research Laboratory's Network Pump (NP).

C. THE NETWORK PUMP (NP)

As with any IT investment, it is important to remember that there is no Holy Grail of IT that can solve all problems. The NP is no different; instead it is one of the key components for a proposed security architecture. When analyzing security architecture there are two major concepts:

- Prevent intrusion of unauthorized entities (e.g. virus, access controls, etc.)
- Prevent unauthorized information flow between computers.

This second concept is where the NP fits into the architecture. In concept, using the Bell-La-Padula (BLP) model, low-level systems should pass information to high-level systems, but high-level systems should not be able to pass information to low-level systems [Ref. 2].

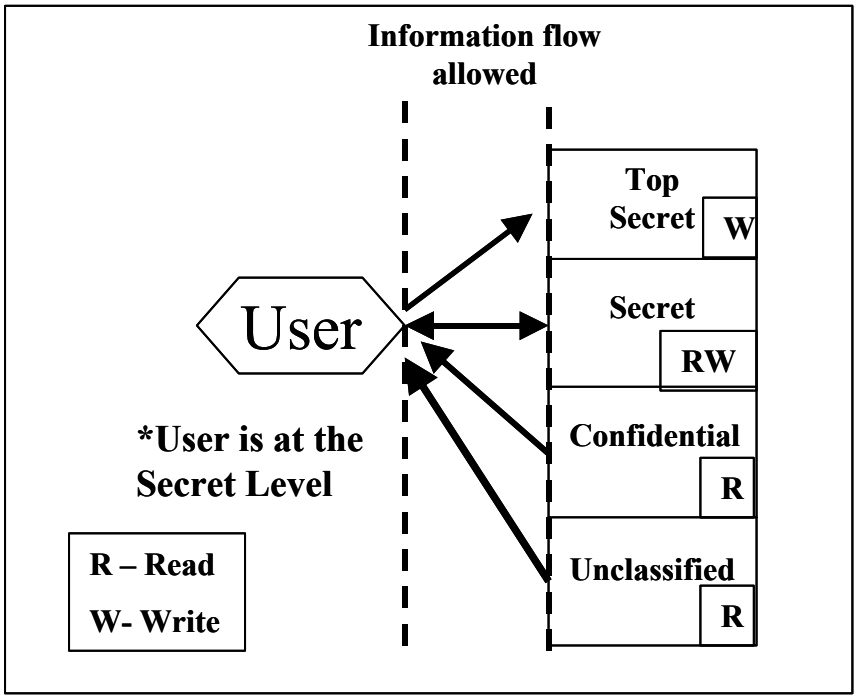

Figure 1. Bell and LaPadula (BLP) Model

This should be easy to implement. In actuality, though, this is a difficult concept to enforce. For example, when a low-level system sends information to high-level one several things could happen. First, because "high" cannot send information down, "low" never knows if high received the message. It is also possible for low to send information too fast for high to handle and overflow high's buffer, leading again to lost information. If high were allowed to send an acknowledgment to low we have violated the security policy and opened up a communication channel that can be exploited. The NP provides one solution to this problem. By controlling acknowledgments, the NP provides both systems with increased reliability and performance, and ensures confidentiality, integrity and authenticity, while preventing the creation of a covert channel.

It does this by receiving a 'wrapped' low-level message into its buffer and then, using a mathematical algorithm, generating an acknowledgement signal based upon probabilistic times. It uses a moving average of the past high acknowledgment times, and sends it to the low system. It also sends the message to the high system and receives an acknowledgment from high to verify receipt of the message. The low system will not send another message until it receives acknowledgment (from the NP) for the last

message it transmitted. The users on both ends will need to login to the NP using a username and password controlled by the NP residing on the high side [Ref. 3].

D. BENEFITS OF THE NETWORK PUMP

The NP is a component that most people, crossing platforms for processing classified information, would say is long in coming. The NP provides for Direct, Indirect and Infrastructure benefits.

1. Direct Benefits

- Reduction in time: Personnel will be able to utilize their time better since they are not performing all the steps previously stated for processing information.
- Reduction in Material: The numerous disks required for moving data from one medium to the next are no longer required.
- Reduction in costs: Initially the NP will cost money, but the costs saved on disks and man-hours will offset the investment.
- Reduction in processing of classified material: Depending on the level of classification for the material, the material will need to be accounted for and held in a secure location. The NP takes the place of the disks, reducing both the generation of classified material and the need to account for the disk originally being used to transfer data.

2. Indirect Benefits

- Improve Customer service: A user will be able to compile information more quickly, providing a product with all the information in one document/disk/file.
- Eliminate the inadvertent violation of computer ethics: many times a user will inadvertently take a classified disk and insert it into an unclassified work station, upload information and then place it back into a classified work station. (No classified disk can be placed in an unclassified system without changing the classification of the system).

3. Infrastructure Investment Benefits

- Reduction in time to provide a desired output (Brief, Intelligence report, consolidation of requirements, etc.): If the user can do it all from one terminal he/she can save time and get the required product out sooner, providing a better service by the organization to the customer.
- Adding flexibility: The NP can be a flexible component allowing a workstation to transfer from a low-level system to a high-level system or allowing a high-level system to receive data across compartment boundaries.

E. DEPARTMENT OF THE NAVY INFORMATION TECHNOLOGY ALIGNMENT

The first question to answer, when deciding whether to invest in the NP, is whether it aligns with DoN strategy concerning IT? According to the DoN Information Management and Information Technology Strategic Plan for FY 02-03 [Ref 4] It's mission is to put information to work for our people. In order to accomplish this mission the DoN has established eight goals and associated objectives quoted below [Ref. 4]:

1. Provide an interoperable information technology infrastructure that ensures knowledge superiority.

2. Infuse advanced information technology into war-fighting and business processes.

3. Maximize the value and manage the risk associated with information technology investments.

4. Proactively encourage the creation and sharing of knowledge to enable effective, timely, and agile decision-making.

5. Exploit emerging information technologies to achieve information dominance.

6. Ensure information resources and critical infrastructures are secure and protected.

7. Build IM/IT competencies to shape the workforce of the future.

8. Foster and incentivize a technology-enabled and information-rich culture.

The NP is well aligned with all of the goals that are not related to creating culture. As discussed earlier, a key component of information/knowledge superiority is the security of our information and communications systems. This leads to increased mission readiness and enhanced organizational effectiveness and efficiency, addressing goals 1, 2, 3, and 6. By investing in the NP we are able to directly increase the security of our information.

We are also able to support goals 4 and 5 by taking advantage of the newest and most technically advanced commercial systems because smaller, trusted devices will ensure our security.

The NP provides a viable secure solution to a complicated problem. The NP will enable users to conduct analysis and compilation of data more efficiently, while providing a more timely delivery of a desired product. The NP enables alternatives to moving data whether from a low-level system to a higher one or across compartments within a security level. However, the key to incorporating any system into an organization is to ensure that the system or component falls within the organizations strategic plan and enhances the productivity of the user, providing a more efficient process of conducting operations securely.

F. IMPLEMENTATION OF THE NP

To incorporate the NP into the DoD infrastructure it is necessary to get the NP through the hurdle of Certification and Accreditation. The NRL has produced and provided many useful documents for the C&A of the NP, but the key requirement for Certification and Accreditation is the creation of a Protection Profile (the end user requirements for a component) and an understanding of the DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) requirements and process.

In the fall of 2001 the Department of the Navy sent out guidance for IT systems, stating that all systems will be certified and accredited [Ref. 5]. The minimum assurance requirement for a component will be C3 (from the TCSEC) or EAL 3 (from the Common Criteria). Prior to October of 2002, the Certification and Accreditation guidance was provided by DoD instruction 5200.28 which required systems to be accredited using the DITSCAP and components using the TCSEC. On October 26, 2002, DoD Instruction 8500.1 cancelled DoD Instruction 5200.28, [Ref. 6], and shifted component certification requirements from the TCSEC standard to the common criteria. Chapter Two will take a close look at the TCSEC as compared to the Common Criteria and a comparison and contrast of the evaluation assurance level of EAL 5 with the TCSEC B2. It will also provide an analysis of the changes that effect the DITSCAP documentation and requirements.

The thesis has two goals:

- To create a Protection Profile for the NP. This will identify the security functions applied to the security-related vulnerabilities, threats and objectives to address the threats.
- To identify correct approaches to certify and accredit the NP within DoN, utilizing the latest documentation.

The purpose of this study is to explore the Certification and Accreditation process as defined by the Department of Defense, and identify applicable metrics for analyzing a specific piece of equipment for Certification and to evaluate its security level and its ability to integrate securely with other systems. The study is intended to identify the security functions from the Common Criteria, which will be used to evaluate the NP. This study will also provide a draft Type SSAA for Certification and Accreditation of the NP.

The thesis will document changes in the DITSCAP that redefine what is required for systems and components for certification and accreditation. We will address the following question:

What is the certification process required for the NP in selected environments, and what is the appropriate certification plan by which to implement the process?

We will also address the following supporting questions:

- What is the NP, and what is the Protection Profile required to securely incorporate the NP in an operational environment?
- Based on the current DITSCAP, and Navy Information Assurance documents, what certification and accreditation requirements apply to the NP in shipboard environments?
- What security assurances must be implemented in order to authorize the NP for use in a selected environment?
- If the NP is to be integrated into a system, what factors will impede successful implementation of the NP and how can these obstacles be overcome?

G. SUMMARY

Currently the Navy operates information systems at many system security levels. Because of the rapidly changing technology and the proliferation of COTS/GOTS hardware and software, the Navy, DoD, and other Federal Agencies find themselves

facing a dilemma of how to enforce their unique security policy requirements while still taking advantage of COTS/GOTS products. The NP was developed to overcome the drawbacks of creating a customized information system and private industry's lack of incentive to produce an information system that meets DoD standards. The NP provides a small, relatively inexpensive component that can be used with COTS technology to enable data transfers from low to high security levels and across compartmental boundaries, while enforcing DoD security policies.

II. LITERATURE REVIEW

A. INTRODUCTION

In order to understand what is involved in documentation for Certification and Accreditation of the NP, we review here the following documents: DoD Trusted Computer System Evaluation Criteria, Common Criteria, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and Information Assurance. This first part of the literature review provides an understanding of the evaluation criteria required to assess the NP for given environments. We look at the existing criteria as outlined in the "Rainbow Series" security classification documentation as the previously accepted DoD criteria and then it will look at the new Common Criteria. The Common Criteria is the future evaluation criteria for systems and components. After presenting the two criteria, we present a comparison on the specific level (EAL 5) at which the NP will be evaluated. Following this the DoD IA policy and DITSCAP are reviewed, as a basis for discussion in Chapter IV [Ref's. 7, 8, 9, 10].

B. TRUSTED COMPUTER SECURITY EVALUATION CRITERIA

The National Computer Security Center is responsible for the Trusted Computer Security Evaluation Criteria (TCSEC) that are incorporated in the "Rainbow Series." This review includes the TCSEC (DoD 5200.28-STD), Interpretation of The TCSEC (NCSC-TG~05), and the DoD TCSEC in Specific Environments (CDC-STD~03-85). These documents identify the minimum security protection required in different network environments.

1. System Security Environments

There are two security environments to consider when identifying which system evaluation criteria to use:

- Closed Security Environment
- Open Security Environment

The Closed Security Environment defines an environment in which the application developers have sufficient clearance and authorization to provide an acceptable presumption that they have not introduced malicious logic, and in which the configuration control provides sufficient

> assurance that the applications are protected against introduction of malicious logic prior to and during the operation of system applications [Ref. 7].
>
> An Open Security Environment is one in which system applications are not adequately protected against the insertion of malicious logic. It includes systems in which the application developer does not have sufficient clearance (or authorization) to provide an acceptable presumption that they have not introduced malicious logic. Moreover, for an Open System the configuration control in the open environment does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to ordering the system application. [Ref. 7] (e.g. a non-cleared commercial software programmer for a small public company could introduce a backdoor into software purchased by DoD).

In respect to the NP, the Closed Security Environment is assumed. All personnel involved in the development have sufficient clearance, and those who maintain the NP in the future will be required to have sufficient clearance to access the NP in a given physical location.

2. Security Clearances and Data Sensitivities

For the purpose of this thesis we will use the standard DoD security clearances and data sensitivity classifications: Unclassified (U), Unclassified but sensitive (N), Confidential (C), Secret (S), Top Secret Background Investigation (TS BI), Top Secret Special Background Investigation (TS SBI), One Category (1C) and Multi-category (MC). Detailed Definitions are listed in Appendix B.

3. Structure of the Evaluation Criteria

The system evaluation criteria in the TCSEC are divided into four divisions: D, C, B, and A. The order is established in a hierarchical form, with A being the highest and D being the lowest. Divisions B and C have subdivisions (B3, B2, B1, C2 and C1) to further delineate system evaluation criteria. In order to qualify for a higher division, all of the lower division requirements must be met along with the additional requirements for the applicable division. This analysis will cover the detailed differences of the divisions/subdivisions D, C1, C2, B1, and B2 with a summary of the differences of B3 and A1 [Ref. 11]. The reason for not covering B3 and A1 in detail is because the NP is only being evaluated up to B2. The following is a breakdown of divisions and their requirements:

Division D. Minimal Protection. It contains only one class and is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.

Division C. Discretionary Protection. This division is divided into two classes C1 and C2. Classes in the division provide for discretionary (need-to-know) protection along with accountability.

Class C1. Discretionary Security Protection.

Security Policy - This class requires the security policy of discretionary access control (DAC) that defines and controls the access between named users and objects in the system. Access control lists are used to specify and control the sharing of objects by individuals or defined groups.

Accountability - This class provides accountability through the process of identification and authentication prior to any action being taken by the user on the system. It also requires the system to protect authentication data, so that unauthorized users cannot access the data.

Assurance - The system will provide operational assurance to protect it from external interference or tampering. It will incorporate life cycle assurance through security testing to ensure security mechanisms work as claimed in the system documentation. This testing will assure that there are no means to compromise system security.

Documentation – The documentation will be required to provide a user's guide to describe how the security protection mechanisms work together. The documentation will provide a Trusted Facility Manual to address cautions about the system and privileges that should be controlled when running the system. Test and Design documentation should also be provided to the evaluators to describe the test procedures, how the security mechanisms were tested, and the results of the testing.

Class C2: Controlled Access.

Security Policy – Same DAC policy as C1, but includes object reuse. Under object reuse no information produced by a previous user's actions is to be available to any user that obtains access to an object released back to the system.

Accountability – The same as C1, but is enhanced to include that the system should be able to uniquely identify individual users and associate the user with all auditable actions. The system will also be required to create and maintain an audit trail of accesses to the objects it protects. The audit data shall be protected by the system to limit access to only those who are authorized to review the data. The system will be required to record the following types of information: use of identification and authentication mechanisms, introduction of objects into user's address space (e.g. file open), deletion of objects, actions taken by users and system administrators, and other security relevant events. Each record shall include: date and time of event, type of event, and success or failure.

Assurance – The same as C1, with the additions of the system being able to isolate resources that are subject to access control and auditing requirements. Testing shall include a search for obvious flaws that would allow violation of resource isolation or that would permit unauthorized access to the audit or authentication data.

Documentation – The same as C1, with the additions to include in the Trusted Facility Manual the procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event.

Division B. Mandatory Protection. The system must preserve the integrity of sensitivity labels and use them to enforce a set of mandatory access control (MAC) rules.

Class B1. Labeled Security Protection. Calls for all the requirements for class C2. It will also include an internal statement of a security policy model, data labeling, and MAC over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

Security Policy – The same as C2, but to include labels and label integrity. Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated. When exported by the system, sensitivity labels shall give the system administrator the ability to specify the printable label names associated with human-readable sensitivity labels that represent the sensitivity of the output. This class shall also enforce MAC policy.

Accountability – The same as C2.

Assurance – The same as C2, with the addition of design specifications and verifications. An informal or formal model of the security policy supported by the system shall be maintained over the life cycle of the system along with a demonstration that the model is consistent with its axioms.

Documentation – The same as C2, with the addition that an informal or formal description of the security policy model, enforced by the system shall be available. An explanation must be provided to show that it is sufficient to enforce the security policy.

Class B2. Structured Protection. Calls for all the requirements from B1. It also includes the addition that covert channels be addressed.

Security Policy – The same as B1, with the addition of trusted path. The system shall support a trusted communication path between itself and user for initial login and authentication. Exclusively, a user shall initiate the communication path. For auditing the system shall be able to audit the identified events that may be used in the exploitation of covert storage channels.

Assurance - The same as B1 with the addition of covert channel analysis. The system developer shall conduct a thorough search for covert storage channels and make a determination of the maximum bandwidth of each identified channel. Design specifications and verification must have a formal model of the system security policy to be maintained over the life cycle of the system. Configuration management shall also be in place during the development and maintenance of the system to maintain control of changes to the descriptive top-level specification, other design data, implementation

documentation, source code, the running version of the object code, test fixtures, and documentation.

Documentation - The same as B1 with the following additions: In the Trusted Facility Manual the requirement that the system modules containing the reference validation mechanism shall be identified. In the design documents the additional requirements in the descriptive top-level specification (DTLS) shall be shown to be an accurate description of the system interface. Documentation shall describe how the system implements the reference monitor concept and give an explanation why it is tamper resistant. The documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels, and all auditable events that may be used in the exploitation of known covert storage channels shall be identified. After completion of the covert channel analysis the bandwidth of known covert storage channels, the use of which is not detectable by auditing mechanisms, shall be provided.

Class B3. Security Domains. Calls for all the requirements for Class B2. It must satisfy the reference monitor requirement that it mediate all accesses of subjects to objects, be tamper proof and be small enough for analysis and testing. A security administrator is to be supported by audit mechanisms to signal security-relevant events. System recovery procedures are also required. Finally, the system must be highly resistant to penetration.

Division A. Verified Protection. This division uses formal security verification methods to assure that DAC and MAC are employed in the system and can effectively protect the system. Division A comprises only the class A1.

Class A1. Verified Design. The systems are functionally equivalent to those in Class B2. However, they require greater amounts of documentation to provide assurance starting with the formal model of security policy and formal top-level specification (FTLS) of the design. Also, more stringent configuration management is required [Ref. 12].

4. Risk Assessment

To identify the class evaluation criteria level for a system it is necessary to identify the risk associated between the user and the data. In Table 1, it shows the cross-reference of the Risk Index to the Minimum Security Class.

Risk Index	Security Operating Mode	Minimum Security Class
0	Dedicated	No Minimum Class
0	System High	C2
1	Limited Access, Controlled, Compartmented, multilevel	B1
2	Limited Access, Controlled, Compartmented, multilevel	B2
3	Controlled, Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

(*) The asterisk indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

Table 1. Security Risk Index
(From Ref. 13)

The risk index is derived from the formula

Risk = Rmax – Rmin,

where Rmax is the maximum data sensitivity as shown in Table 2 and Rmin is the minimum user clearance as shown in Table 3. Each data level receives a rating starting with unclassified at 0 and Top Secret (MC) rating of 7.

Minimum User Clearance	Rmax
Unclassified (U)	0
Not Classified but Sensitive	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)	5
Top Secret with One Category (1C) Secret or Top Secret	6
Top Secret with Multiple Categories (MC) Secret or Top Secret	7

Table 2. Rating Schedule for Maximum Data Sensitivity (Rmax)
(From Ref. 13)

Each user clearance is assigned a rating, starting with unclassified users receiving a rating of 0 and multiple category users receiving a rating of 7.

Minimum User Clearance	Rmin
Uncleared or not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Classified Information	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or Background Investigation (BI)	4
Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

Table 3. Rating Schedule for Minimum User Clearance (Rmin)
(From Ref. 13)

Tables 4 and 5 show the cross-reference to obtain the risk based on the Risk Index formula.

		Maximum Data Sensitivity						
Minimum Clearance or Authorization of System Users		U	N	C	S	TS	1	MC
	U	0	1	2	3	4	5	6
	N	0	0	1	2	4	5	6
	C	0	0	0	1	3	4	5
	S	0	0	0	0	2	3	4
	TS(BI)	0	0	0	0	0	2	3
	TS(SBI)	0	0	0	0	0	0	2
	1C	0	0	0	0	0	0	1
	MC	0	0	0	0	0	0	0

Table 4. Security Risk Index Matrix
(From Ref. 13)

		Maximum Data Sensitivity						
Minimum Clearance or Authorization of System Users		U	N	C	S	TS	1	MC
	U	C1	B1	B2	B3	*	*	*
	N	C1	C2	B2	B2	A1	*	*
	C	C1	C2	C2	B1	B3	A1	*
	S	C1	C2	C2	C2	B2	B3	A1
	TS(BI)	C1	C2	C2	C2	C2	B2	B3
	TS(SBI)	C1	C2	C2	C2	C2	B1	B2
	1C	C1	C2	C2	C2	C2	C2	B1
	MC	C1	C2	C2	C2	C2	C2	C2

(*) The asterisk indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

Table 5. Security Risk Index Matrix
(From Ref. 13)

In the majority of calculations for assessing the risk index for the NP, the risk index is 0. The data is always at a lower classification level than the user's clearance. As Table 1 shows, the class level of C2 correlates with a risk index of 0. The higher class of B2 is required when the NP is used in a compartmentalized environment and used for Multiple Categories with possible users in the physical environment being cleared only for TS (SBI). The data maintains the same security level, but not all personnel have the need to know within the secure environment.

C. THE COMMON CRITERIA

The Common Criteria was developed to provide an international standard for evaluation of IT security. Personnel involved in its development were from Canada, Europe, and the United States. The goal was to incorporate the Canadian Criteria (CTCPEC), European Criteria (ITSEC), and the United States Criteria (TCSEC) into one document. The Common Criteria provides for a standard that enables systems to be evaluated, compared, and certified under the same requirements. This in turn increases the ease of integration of subsystems by allowing network administrators to cross reference security evaluations. It ensures that the components integrated meet the desired level needed to maintain the system assurance level [Ref. 8].

Version 1.0 of the Common Criteria was published in January 1996, and Version 2.0 was published in 1998. Version 2.0 was accepted by the International Organization for Standards (ISO) as a Final Committee Draft (FCD), and formally accepted in 1999. The overall purpose of the Common Criteria is to provide the guidance for certification and accreditation for a component or system at a given Evaluation Assurance Level (EAL). The Common Criteria is divided into three parts:

- Part 1 - Introduction and General Model
- Part 2 – Security Functional Requirements
- Part 3 – Security Assurance Requirements.

There is also a supporting document of Common Evaluation Methodology divided into two parts (CEM 1 and 2) still in version 1.0 [Ref. 8].

This review will focus on Part 3: Security Assurance Requirements. The goal is to understand the EALs as the NP is being evaluated for an EAL 5 level of assurance.

1. The Evaluation Assurance Levels (EALs)

EALs are evaluation classes that provide an increasing scale that balances the level of assurance obtained with the cost of feasibility of acquiring that degree of assurance. There are seven EALs (EAL1-EAL7) in a hierarchical structure with EAL 1 being the lowest and EAL7 being the highest. Each incremental EAL contains all the requirements of the preceding lower EAL plus its additional requirements for its specific level. Table 6 delineates the requirements for each EAL.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Class ACM: Configuration Management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Class ADO: Delivery and Operation	ADO_DEL	1	1	2	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Class ADV: Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Class AGD: Guidance Documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Class ALC: Life cycle Support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Class ATE: Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Class AVA: Vulnerability Assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6. Evaluation assurance level summary
(From Ref. 8)

To use this table the user looks for the desired EAL (top row) and crosses it with the Assurance Class in the far left column. The numbers in the matrix indicate the level of the Assurance Class that must be obtain to qualify for the specific EAL. The increasing number represents more stringent requirements. Each EAL increase is directly proportional to the increasing numbers in the matrix.

Example: To identify the Tests required for an EAL 3 rating the user would find EAL 3, cross with the Assurance Class of Class ATE (Tests), and identify that there are four Assurance Families associated with its testing requirements. Each of the four Assurance Families has a specific test requirement to be met. Looking at Table 6 the first test requirement of ATE_COV requires the 2nd level of ATE_COV (ATE_COV.2). The breakdown of all the Assurance Family requirements can be found at http://www.commoncriteria.org/part3.htm (The Assurance Family requirements incorporate approximately 200 pages of detailed description in Part 3 of the Common Criteria which would be too lengthy to be of use for this review).

A closer look at the increasing requirements EALs is as follows:

EAL 1 – Functionally Tested. This is required when some confidence in correct operation is required, but threats to security are not viewed as serious. Table 7 indicates the requirements for EAL 1.

Assurance class	Assurance components
Class ACM: configuration Management	ACM_CAP.1 Version numbers
Class ADO: Delivery and Operation	ADO_IGS.1 Installation, generation, and start-up Procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_IND.1 Independent testing – conformance

Table 7. EAL 1 Requirements
(From Ref. 8)

EAL 2 – Structurally Tested. This is required when low to moderate levels of independently assured security requirements are needed in the absence of readability of the complete development record. Table 8 indicates the requirements for EAL 2.

Assurance class	Assurance components
Class ACM: Configuration Management	ACM_CAP.2 Configuration items
Class ADO: Delivery and Operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability Assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 8. EAL 2 Requirements
(From Ref. 8)

EAL 3 – Methodically Tested and Checked. This is required when a moderate level of independently assured security is needed. This level requires a thorough investigation of the system and its development without incurring substantial re-engineering costs. It also requires development environment controls and configuration management. Table 9 indicates the requirements for EAL 3.

Assurance class	Assurance components
Class ACM: Configuration Management	ACM_CAP.3 Authorization controls
	ACM_SCP.1 TOE CM coverage
Class ADO: Delivery and Operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle Support	ALC_DVS.1 Identification of security measures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability Assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 9. EAL 3 Requirements
(From Ref. 8)

EAL 4 – Methodically Designed, Tested and Reviewed. This is required when a moderate to high level of independently assured security is needed. It is requires testing by an independent search for obvious vulnerabilities. It requires development controls supported by a life cycle model and automated configuration management. Table 10 indicates the requirements for EAL 4.

Assurance class	Assurance components
Class ACM: Configuration Management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Class ADO: Delivery and Operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle Support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

Table 10. EAL 4 Requirements
(From Ref. 8)

EAL 5- Semi-formally Designed and Tested. This is required for a high level of independently assured security, in a planned development. It requires a formal model, a semi-formal presentation of the functional specification, and high level design and a semi-formal demonstration of correspondence. An independent search for vulnerabilities is also required to include assurance of resistance to a penetration attacker with moderate attack potential, covert channel analysis and modular design. Table 11 indicates the requirements for EAL 5.

Assurance class	Assurance components
Class ACM: Configuration Management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.3 Development tools CM coverage
Class ADO: Delivery and Operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.3 Semiformal functional specification
	ADV_HLD.3 Semiformal high-level design
	ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Modularity
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.2 Semiformal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle Support	ALC_DVS.1 Identification of security measures
	ALC_LCD.2 Standardized life-cycle model
	ALC_TAT.2 Compliance with implementation standards
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: low-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_CCA.1 Covert channel analysis
	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.3 Moderately resistant

Table 11. EAL 5 Requirements
(From Ref. 8)

EAL 6- Semi-formally Verified Design and Tested. This is required for high-risk situations where the value of the protected assets justifies the additional cost. It requires the system to have a modular and layered approach to design. It also requires an independent search for vulnerabilities that must include a systematic search for covert channels and the development environment and configuration management are further strengthened. Table 12 indicates the requirements for EAL 6.

Assurance class	Assurance components
Class ACM: Configuration Management	ACM_AUT.2 Complete CM automation
	ACM_CAP.5 Advanced support
	ACM_SCP.3 Development tools CM coverage
Class ADO: Delivery And operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures

Assurance class	Assurance components
Class ADV: Development	ADV_FSP.3 Semiformal functional specification
	ADV_HLD.4 Semiformal high-level explanation
	ADV_IMP.3 Structured implementation of the TSF
	ADV_INT.2 Reduction of complexity
	ADV_LLD.2 Semiformal low-level design
	ADV_RCR.2 Semiformal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle Support	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Standardized life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
Class ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.2 Testing: low-level design
	ATE_FUN.2 Ordered functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_CCA.2 Systematic covert channel analysis
	AVA_MSU.3 Analysis and testing for insecure states
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.4 Highly resistant

Table 12. EAL 6 Requirements
(From Ref. 8)

EAL 7 – Formally Verified Design and Tests. This is required for systems in extremely high-risk situations. It requires a formal model supplemented by a formal presentation of the functional specification and high-level design. The developer must provide "white box" testing and the system must undergo complete independent confirmation of developer's test results. Also, the complexity of the design must be minimized. Table 13 indicates the requirements for EAL 7.

Assurance class	Assurance components
Class ACM: Configuration Management	ACM_AUT.2 Complete CM automation
	ACM_CAP.5 Advanced support
	ACM_SCP.3 Development tools CM coverage
Class ADO: Delivery and Operation	ADO_DEL.3 Prevention of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.4 Formal functional specification
	ADV_HLD.5 Formal high-level design
	ADV_IMP.3 Structured implementation of the TSF
	ADV_INT.3 Minimization of complexity
	ADV_LLD.2 Semiformal low-level design
	ADV_RCR.3 Formal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model

Assurance class	Assurance components
Class AGD: Guidance Documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle Support	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.3 Measurable life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
Class ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.3 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
Class AVA: Vulnerability Assessment	AVA_CCA.2 Systematic covert channel analysis
	AVA_MSU.3 Analysis and testing for insecure states
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.4 Highly resistant

Table 13. EAL 7 Requirements
(From Ref. 8)

2. Backward Compatibility and Legacy Application

Environment EALs outlined in the Common Criteria do not cross EALs to a risk index for evaluating which physical environment the EALs should be used in (Unclassified through Multi-categories). What it provides is a cross-reference table of what EALs are equivalent to class criteria in the United States' TCSEC and the European ITSEC. Table 14 is incorporated in the Common Criteria to provide backward compatibility for legacy systems. It also ensures the results of previous evaluations remain relevant [Ref. 8].

Common Criteria	US TCSEC	European ITSEC
-	D: Minimal Protection	E0
EAL 1	-	-
EAL 2	C1: Discretionary Security Protection	E1
EAL 3	C2: Controlled Access Protection	E2
EAL 4	B1: Labeled Security Protection	E3
EAL 5	B2: Structured Protection	E4
EAL 6	B3: Security Domains	E5
EAL 7	A1: Verified Design	E6

Table 14. Criteria Evaluation Cross Reference
(From Ref. 8)

D. COMPARISON OF B2 AND EAL 5

Since the NP is being evaluated for use in various physical environments, from unclassified to multi-categories, the TCSEC requires the minimum assurance of B2 that

crosses over to the desired level of EAL 5 outlined in the Security Target for the NP. Therefore, it is necessary to carefully compose TCSEC B2 and Common Criteria EAL 5 requirement.

After reviewing the criteria of Class B2 and the detailed Assurance Families of EAL 5 the results are as follows, broken down using the Assurance Classes of the Common Criteria:

Design – Both require formal models.

Configuration Management (CM) – B2 requires stringent CM while EAL 5 requires the CM to be partially automated.

Delivery and Operations – B2 does not include delivery requirements while EAL 5 requires controls to ensure that component is delivered to the user without any changes throughout the system.

Development – For B2, the design documentation is to be top-level system architecture and must include a security policy of DAC and MAC, while EAL 5 requires the design documentation to be high-level and include a formal security policy. All other aspects are the same.

Guidance – For B2, the guidance is outlined using the Trusted Facility Manual (TFM) and the Security Functional User Guide (SFUG). EAL 5 requires all guidance to be provided to the users and system administrators, not necessarily designating a specific common publication.

Life Cycle Support - B2 requires the life cycle support to be included in the TFM, while EAL 5 only requires that documentation be provided. The larger difference between the two lies in testing. B2 requires that all flaws identified in the evaluation be corrected and retested to ensure that the corrections do not cause any more flaws. EAL 5 requires flaws to be identified.

Vulnerability Assessment – B2 requires that the developer conduct covert channel analysis and identify the maximum bandwidth for each channel. EAL 5 requires an independent penetration test and covert channel analysis, but does not require the identification of the maximum bandwidth for each channel.

Table 15 below summarizes the differences between TCSEC B2 and Common Criteria EAL 5.

Class	Component	TCSEC B2	EAL5
Design	Formal Model	X	X
Configuration Management	Stringent Control	X	
	Partially Automated		X
Delivery	Prevent Changes in Route		X
	Not Specified	X	
Development	Top Level	X	
	High Level		X
	DAC	X	Through SFR
	MAC	X	Through SFR
Guidance	TFM	X	
	SFUG	X	
	Some form of Guidance in any format		X
Life Cycle Support	Life Cycle support listed in TFM	X	
	Provided in some form of Documentation		X
	Flaws Identified and Fixed	X	
	Flaws Realized (Identified)		X
Vulnerability Assessment	Developer Conduct Covert Analysis	X	
	Independent Penetration Test		X
	Independent Covert Analysis		X
	Identify Bandwidth	X	

Table 15. TCSEC-B2 Summary Comparison

Other areas of interest to assess which evaluation system should be used to classify the NP are as follows: For B2 the TCSEC identifies stringent labeling requirements for marking the output of the system. The TCSEC also discusses the requirements for object reuse and the implicit requirements for DAC and MAC. For EAL 5 there is no discussion on labeling, object reuse or DAC/MAC Policy. However the security functions in the Common Criteria give the User, Developer and the Evaluator requirements the component must meet to address the threats and objectives relative to the threats. The Security Functions are delineated in the Protection Profile (user's requirements for a given component) and/or the Security Target (developer's answers to meeting the goals of the Protection Profile) if the Common Criteria is used.

The new DoDD 8500.1 specifies that all systems will be certified and accredited using a NSA (National Security Agency) approved method, and components will be

Certified and Accredited using the Common Criteria (which is an approved NSA method) [Ref. 6]. Therefore, we will evaluate the NP to meet the Common Criteria EAL 5 level. By choosing the EAL 5, the NP will qualify as a GOTS device that can be incorporated into many existing, and systems requiring an evaluation up to an EAL 5.

Using the Common Criteria EAL 5 method of evaluation also allows the NP to be evaluated under less constraining requirements than the TCSEC B2, but still addressing all threats and security objectives identified to overcome the threats. The TCSEC was written to provide specific requirements in certification and accreditation of a component or system. The Common Criteria's intent was to provide a broader set of requirements to be more adaptable over a larger range of components and systems. Although, there are specific Assurance class requirements within the Common Criteria, it is up to the implementation of the Security Function Requirements (SFRs) as they are applied to support the identified threats and objectives for the certification of a component. Not all components require the same specific functions (i.e. MAC, Mail, etc); therefore implementing the pertinent SFRs allows a component to be certified appropriately and without the need to identify exceptions.

The next part of this review analyzes, the DITSCAP criteria with respect to certifying and accrediting the NP to be used aboard ships.

E. INFORMATION ASSURANCE

The Department of Defense Directive 8500.1 dictates policies to achieve Information Assurance through a defense-in-depth approach that incorporates the capabilities of personnel, operations, and technology. It applies to all DoD owned or controlled information systems that receive, process, store, display, or transmit DoD information regardless of mission assurance category, classification, or sensitivity. All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that is a balance among sensitivity of the information, documented threats and vulnerabilities, trustworthiness of users and interconnecting systems, the impact of disruption or destruction to the DoD information system and cost effectiveness.

The 8500.1 also states that interconnections among DoD information systems of different security domains or with other U.S. Government systems of different security domains shall be employed only to meet compelling operational requirements, not for operational convenience. Because of the NP's functionality as a guard, interconnecting information systems of different security domains brings it into direct conflict with the 8500.1 except in the rare cases where compelling operational requirements are proven. This conflict could significantly jeopardize the possible benefits brought to the fleet by interconnecting information systems of different security domains for operation convenience such as reduced system costs, greater functionality, improved efficiency, centralized access to data, and the promotion of communication and cooperation. For this thesis, we assume that the intent of this statement in the 8500.1 is meant for crossing different security agency boundaries. If this is not the case then the fleet will never be able to use the NP to connect the SIPR and NIPR nets because it will not meet the compelling operational requirement, but instead fall under the operational convenience category.

Finally, the 8500.1 directs the requirements for component and system certification. All Information Assurance products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11, of which the Common Criteria is part. Once compliance is verified, all DoD information systems shall be certified and accredited in accordance with the DITSCAP.

F. DITSCAP

The DITSCAP is the standard Certification and Accreditation process for the Department of Defense. It provides a detailed approach to the activities compromising the C&A process leading to accreditation and establishes a process and management baseline. It establishes a standard process, set of activities, tasks, and a management structure to certify and accredit Information Systems and security postures of the Defense Information Infrastructure (DII). The principal purpose of the process is to protect and secure the DII with a proper balance between the benefits to the operational mission, the risks to those same missions, and life-cycle costs. Standardizing the process helps to ensure the shared interests are represented and accounted for in the decision making

process. Tailoring of the DITSCAP to fit the size and complexity of the system and the required level of IA is authorized, but each phase shall be accomplished.

The DITSCAP consists of four phases: Definition, Verification, Validation, and Post-Accreditation. The definition phase includes activities to verify the system mission, environment and architecture, identify the threat, define the levels of effort, identify the Designated Approving Authority (DAA) and Certification Authority, and document the C&A security requirements. This phase culminates with a documented agreement between the DAA, Certifier, and user representatives on the approach and results of phase one activities. The verification phase includes activities to document compliance of the system with previously agreed upon security requirements. For each life-cycle development activity, a corresponding set of security activities verifies compliance with the security requirements and constraints and evaluates vulnerabilities. The validation phase includes activities to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk. Validation culminates in an approval to operate. The post accreditation phase includes activities to monitor system management, configuration, and changes to the operational threat environment to ensure an acceptable level of residual risk is preserved. This phase includes periodic security management, configuration management, and compliance validation reviews. Changes to the system environment or operations may warrant beginning a new DITSCAP cycle.

During the DITSCAP cycle, the certification portion is a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process. It establishes the extent to which a particular design and implementation meets a set of specified security requirements. The technical security features evaluate and establish the extent to which a particular design meets a set of specified security requirements with respect to the INFOSEC measures of COMPUSEC, COMSEC, and EMSEC. This assessment is done against a developed product. A Type Certification allows the effort to be performed once, independent of specific implementation, and the results reused many times. The non-technical security features evaluate and establish the extent to which a particular implementation meets a set of specified security requirements with respect to the

INFOSEC measures of PHYSEC, PERSEC, PROSEC, and SETA. This assessment is against a product implemented in an operational environment called an Operational Site Certification.

The accreditation portion includes a formal declaration by a DAA that a site or an information system is approved to operate in a prescribed operational configuration using a defined set of safeguards and countermeasures against stated threats and vulnerabilities. Upon completion of the accreditation process, the DAA may take one of the following actions:

- Accredit the system to process information in the given operational environment.
- Issue an Interim Authority To Operate (IATO) when the DAA determines changes are needed to the system or its environment, but the system will operate in the interim. An IATO may not exceed one year.
- Reject accreditation and recommend enhancements that will lead to accreditation.
- Reject accreditation because of inherent security deficiencies and provide rationale.

Throughout the DITSCAP, all of the information relevant to the C&A is collected into one document, the Systems Security Authorization Agreement (SSAA). The SSAA is a living document that is produced at the completion of the definition phase and continuously updated and incorporated into a Site SSAA. The Site SSAA is reviewed periodically or whenever there is a change to the information system. Characteristics common to SSAAs are:

- Description of the operating environment and threats.
- Description of the component/system architecture.
- Establishment of the C&A boundary of the system to be accredited.
- Documentation of the formal agreement among the DDAA or DAA, Certifier, User Representative, and Program Manager.
- Documentation of all requirements necessary for accreditation.
- Documentation of all security criteria for use throughout the IS lifecycle.
- Minimization of documentation requirements by consolidating applicable information into the SSAA.

- Documentation of the DITSCAP plan.
- Documentation of test plans and procedures, certification results, and residual risk.
- The SSAA contributes the baseline security configuration document.

In Chapter III a formal development of the protection profile used to accomplish the technical certification of the NRL NP is developed. Chapter IV then discusses the steps necessary to complete phases one, two, and three of the DITSCAP and provides an SSAA template for the NP.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK PUMP PROTECTION PROFILE

A. INTRODUCTION

To Facilitate the Certification and Accreditation (C&A) of the NP, we have employed the Common Criteria to provide the guidance and direction necessary to meet or exceed the requirements for the NP at a rating of EAL 5. The C&A using the Common Criteria requires two specific documents to be provided to the evaluator (certifier): the Protection Profile and the Security Target. The Protection Profile is a user-generated document (further described in para. 3.B.) that outlines the user's requirements for meeting all security requirements for a given assurance level. The Security Target is the developer's document that addresses all aspects of the Protection Profile to ensure the component is meeting the requested security requirements and ensures the user's desires are met. This chapter describes in more detail what a Protection Profile is, compare and contrast three Protection Profiles reviewed to create the NP Protection Profile, and describe the Protection Profile we have created for the NP.

The Security Target can be found at [Ref. 14]. It was developed by NRL for use in certifying the NP.

This chapter also provides a comparison and contrast of the Controlled Access Protection Profile (CAPP) [Ref. 15], the Labeled Security Protection Profile (LSPP) [Ref. 16], and the DoD Mail Guard for High Robustness Environments Protection Profile (MGHREPP) [Ref 17], which were the profiles used in creating the NP Protection Profile. A brief description of each Protection Profile is as follows:

- CAPP – This Protection Profile is for a set of security-functional and assurance requirements for Information Technology products. The components for CAPP support access controls that are capable of enforcing access limitations on individual users and data objects. CAPP provides a level of protection that is appropriate for a non-hostile and well-managed user community requiring protection against threats and inadvertent or casual attempts to breach system security [Ref. 15].
- LSPP – This Protection Profile is for a set of security-functional and assurance requirements for Information Technology products. The components for LSPP support access controls capable of enforcing access limitations on individual users and data objects. Specifically, two classes of access controls are provided:

- Those that allow individual users to specify how resources under their control are to be shared.
- Those that enforce limitations on sharing among users (Labeling).

The LSPP does not fully address the threats posed by malicious system development or administrative personnel. [Ref. 16].

- MGHREPP –This Protection Profile is for a Mail Guard that sits between two protected network enclaves at different classification levels, controlling the flow of electronic messages sent between the two networks. The guard employs various processing, filtering, and data-blocking techniques in an attempt to provide data sanitation or separation between enclaves. The guard provides identification and authentication, trusted path and audit capabilities, providing services for confidentiality and integrity of mail messages [Ref. 17].

B. WHAT IS A PROTECTION PROFILE?

1. Definition and Use

A Protection Profile is an independent document that states the security requirements that address the threats that exist in a specified environment. A Protection Profile could be used by a consumer group, government agency, or an organization that wishes to specify security requirements for an application type, a component, a class of security product, or an IT system.

Using the Protection Profile concept, similar products can be evaluated using an existing Protection Profile for their security requirements or use a Protection Profile that is close to its function, tailoring it to reduce the effort. Protection Profiles reduce the need to reinvent the process for like applications, components, etc.

2. Protection Profile Breakdown

As described in [Ref. 8], the Protection Profile is broken down into six sections: Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, and Rationale.

- Section One provides overview and the organizational layout for the Protection Profile. It also provides any references to other Protection Profiles.
- Section Two provides a description of the application, component or system being evaluated.

- Section Three describes the expected environment in which the TOE will be used, along with any assumptions that need to be defined. It also defines the set of threats that are relevant to the secure operation of the TOE.
- Section Four defines the set of security objectives required to satisfy the TOE threats.
- Section Five defines the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that are required to be satisfied by the TOE.
- Section Six provides the rationale that the security objectives satisfy the threats and policies. This section also provides the justification of the appropriate security function requirements to satisfy a specific objective [Ref. 8].

C. COMPARISON OF PROTECTION PROFILES

1. LSPP Versus CAPP

The CAPP was written to provide a protection profile for a C2 level of assurance using the recently canceled DoDD 5200.28std. It was also evaluated for an assurance rating of EAL 3 [Ref. 16]. The LSPP was written to provide a Protection Profile for a B1 level of assurance and was also evaluated at an augmented EAL3. The LSPP was derived from the CAPP, using the same Section 1 and Section 2 [Ref. 17]. The key difference between the two is the addition of the Labeling and Mandatory Access Controls (MAC) in the Security Functional requirements of the LSPP. The assurance levels are identical for both PPs. The old Assurance level B1 requires the TOE to provide security labels and also MAC. The security labels and MAC are the augmented portion of the EAL 3 augmented rating that NSA assigned during its validation.

Although the LSPP was being validated for a rating of B1 this is not consistent with the Common Criteria cross reference of the DoDD 5200.28std. The cross-reference states that TOEs evaluated with an existing B1 are equivalent to a rating of an EAL4. The lower rating is related to the lack of documentation in the LSPP Security Functional Requirements and Assurance Level Requirements.

We are writing a Protection Profile for an EAL 5 level component that requires certification and accreditation. Since the LSPP does not address the need for Covert Channel Analysis, it is necessary to look at another existing (draft) Protection profile that

requires covert channel analysis. The protection profile chosen is the MGHREPP [Ref. 17]. The MGHREPP closely resembles the NP and is being evaluated for a rating of an EAL 4+.

2. LSPP Versus MGHREPP

The LAPP was written to address generic TOEs requiring or already having an assurance level of B1. The MGHREPP was written to address all the requirements of the LSPP, covert channel analysis, more formal documentation, and the requirements for a specific TOE [Ref. 17].

Since the two Protection Profiles are different in the end TOE result, it is necessary to break down the differences by section.

Section one of the LSPP does not follow the Common Criteria template, (there is no requirement for the sections to be identical to the Common Criteria guidance. The protection profiles must only meet the minimum for each section.) The LSPP does not include the breakdown of the protection profile for the evaluator, but it does include a paragraph for the strength of environment; that is used to identify the protection profile as an EAL 3 augmented and the Strength of Function as a SOF-medium.

Section Two of the LSPP gives a generic description and summary of the requirements for a TOE that would use the LSPP. The MGHREPP gives a description of a specific mail guard and its proposed architecture. It covers the information flow of the TOE and what security functions it should perform. It also gives a summary explanation for the EAL 4+, which will be discussed in greater detail in the comparison and contrast of Section Six.

Section Three of the MGHREPP identifies the threats it perceives to be addressed in the security functions of the Mail Guard. The LSPP leaves the threat assessment up to the Organization Security Policy. Both protection profiles specify the assumptions for secure usage of the environment of the TOE.

Section Four outlines the security objectives for both protection profiles, however the MGHREPP breaks the objectives down into TOE security objectives and security objectives for the environment in which the TOE will be incorporated. The LSPP breaks the objectives into IT security objectives and non-IT security objectives. Although these

two approaches are different, they both outline the required objectives to be addressed by the security Function Requirements in Section Five.

Section Five of the MGHREPP outlines the security functions that relate to covert channel analysis, importing and exporting data, cryptographic operations, and in-depth formal testing of the TOE. The LSPP, being a generic protection profile, allows for greater flexibility in the security functions required and is written to address the basic security requirements of Discretionary Access Control (DAC), MAC, and security labeling. The LSPP Security Functional requirements do address the exporting and importing of data. The difference is that the LSPP assumes the data is of the same security classification and the MGHREPP processes mail crossing between different classification environments.

The MGHREPP also includes the Security Assurance Requirements in its Section five, where the LSPP makes a new section for the Security Assurance Requirements. Both Assurance sections follow the Common Criteria conventions for the Assurance Classes.

The LSPP follows a straight EAL3 Security Assurance Requirements with the exception of requiring Security Policy Modeling of the TOE. The MGHREPP follows the Common Criteria conventions for an EAL 4 rating, but it requires the TOE to meet the development assurance requirements up to an EAL6 to ensure that the high-level and low-level design are described in a semi-formal manner and are supported by a semi-formal security policy model. The other deviation from the EAL 4 rating is in the Testing and Vulnerability Assessment classes. The requirements must meet an EAL 6 rating to ensure that the functional testing, covert channel analysis, and thorough analysis for vulnerabilities are performed.

Section Six of the MGHREPP and Section Seven of the LSPP provide the rationale that show how the Security Functional Requirements address and achieve the objectives for the TOE. Since both protection profiles use different objectives the two cannot be compared directly. Never the less, each protection profile provides the relationship of Security Functional Requirements to the objectives to ensure all objectives are met as would be expected by any protection profile.

Table 16 below provides a summary comparison between the LSPP and the MGHREPP.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Class ACM: Configuration Management	ACM_AUT					O		
	ACM_CAP			X		O		
	ACM_SCP			X	O			
Class ADO: Delivery and Operation	ADO_DEL			X		O		
	ADO_IGS			X		O		
Class ADV: Development	ADV_FSP			X		O		
	ADV_HLD			X			O	
	ADV_IMP						O	
	ADV_INT						O	
	ADV_LLD						O	
	ADV_RCR			X		O		
	ADV_SPM				X O			
Class AGD: Guidance Documents	AGD_ADM			X		O		
	AGD_USR			X		O		
Class ALC: Life cycle Support	ALC_DVS			X		O		
	ALC_FLR					O		
	ALC_LCD				O			
	ALC_TAT				O			
Class ATE: Tests	ATE_COV			X		O		
	ATE_DPT			X		O		
	ATE_FUN			X			O	
	ATE_IND			X			O	
Class AVA: Vulnerability Assessment	AVA_CCA						O	
	AVA_MSU			X			O	
	AVA_SOF			X			O	
	AVA_VLA			X			O	

Legend: LSPP = X MGHREPP = O

Table 16. Comparison of LSPP and MGHREPP

D. CREATION OF THE NP PROTECTION PROFILE

The Protection Profile can be derived by any of the following:

- Creating a new Protection Profile from scratch, using the guidance provided in the Common Criteria.
- Identifying an existing Protection Profile that matches the uses of the component, application, etc. to be evaluated and using it as the TOE Protection Profile.
- Identifying an existing profile and tailoring it to meet the requirements of the TOE.

The NP Protection Profile was derived from the last. NIAP (National Information Assurance Partnership) maintains a listing of validated, and draft Protection Profiles available for reuse. The NP Protection Profile was tailored from the MGHREPP. The MGHREPP provided the closest applicable use between the CAPP, the LSPP, and the MGHREPP. Although the NP does not require MAC or security labels it does require covert channel analysis and formal documentation. The MGHREPP is a draft Protection Profile, not yet validated by NIAP [Ref. 18].

The following describes how each section of the NP Protection Profile is derived:

Section One is tailored to introduce the NP as a device that will be used in a high robustness environment. It provides the basic introduction of the NP and identifies the key players involved in the initial C&A process.

Section two is taken directly from the Security Target [Ref. 14]. The TOE Functional description from the Security Target is the same as required by the NP Protection Profile.

Section Three's assumptions are that the NP will be installed in a shipboard environment. Three options have been identified for deploying/installing the NP into the ship's network. The options have been incorporated in the current shipboard structure shown in Figure 2.

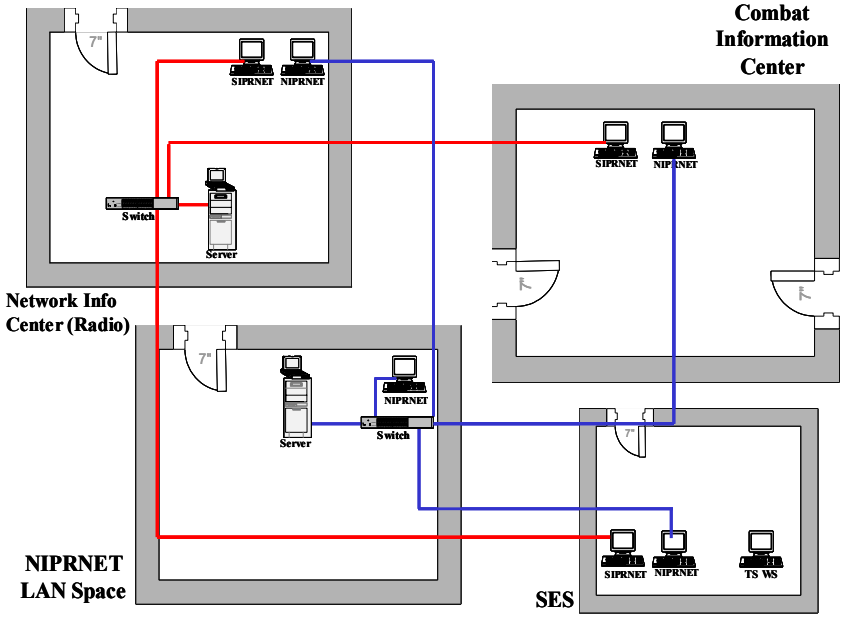

Figure 2. Current Shipboard Environment (DDG 51 Class)

Option 1 incorporates the unclassified LAN (NIPRNET) passing data to the Secret LAN (SIPRNET) as shown in Figure 3.

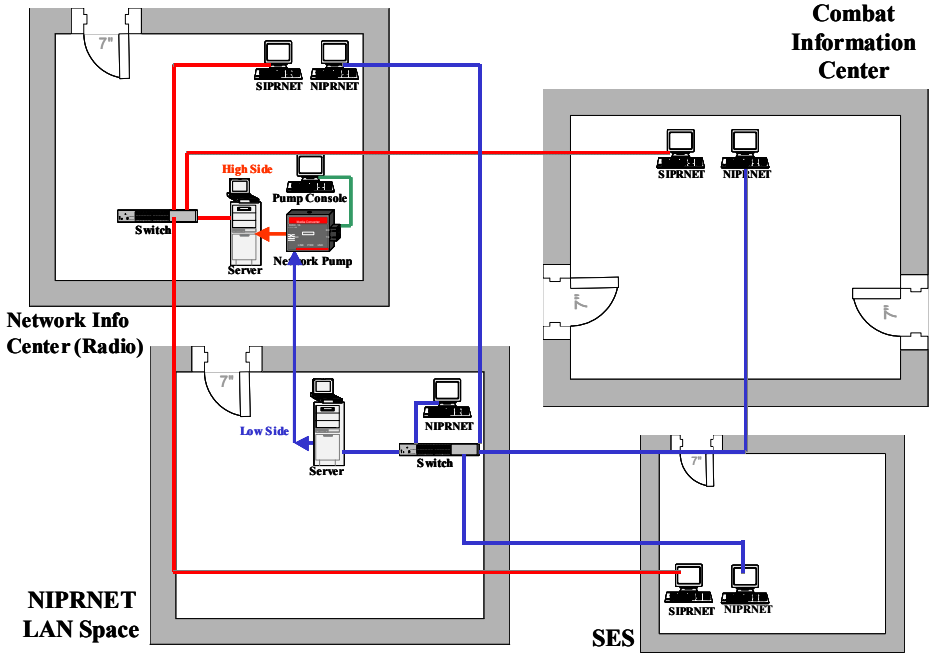

Figure 3. Shipboard Option 1

Option 2 incorporates the installation of two NPs to pass data from the Unclassified LAN to the Secret LAN and then from the Secret LAN to the Top Secret LAN as shown in Figure 4.

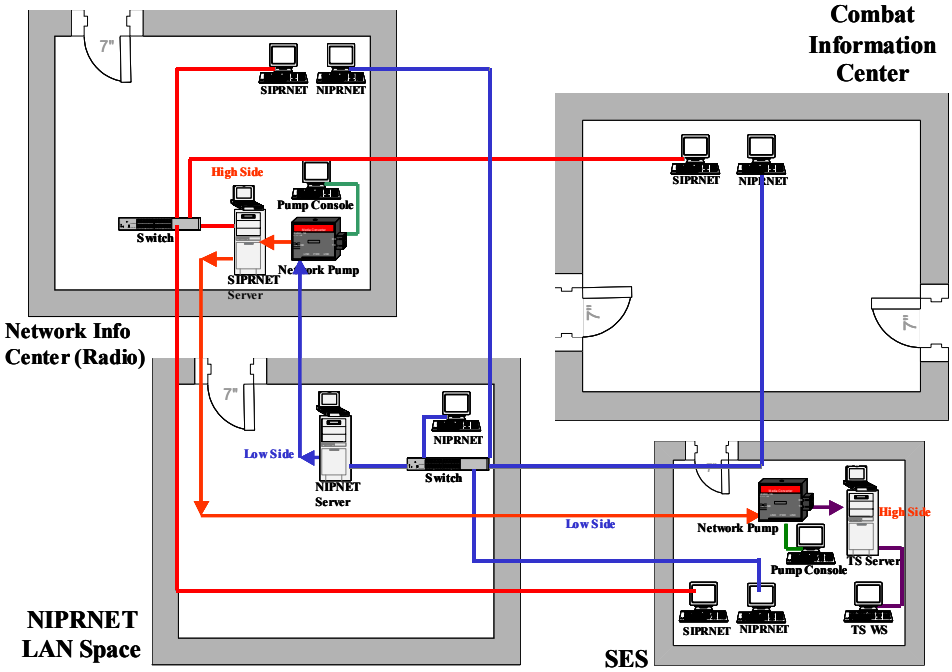

Figure 4. Shipboard Option 2

Option 3 incorporates the installation of one NP to pass data from the Unclassified LAN and the Secret LAN to the Top Secret LAN, concurrently (as shown in Figure 5).

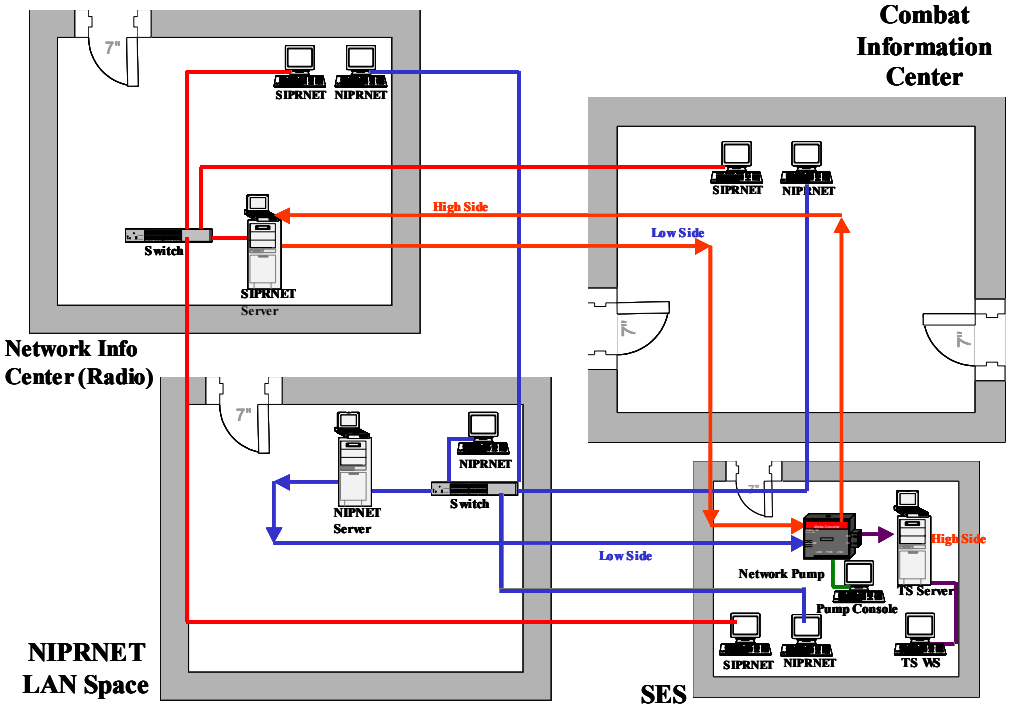

Figure 5. Shipboard Option 3

The Security features assumed for each LAN area are as identified Table 17.

	Physical Security	Personnel Security	Space Rating	Space Location
Unclassified LAN	**All Metal Room** **Cipher Lock** **Pad Lock**	**System Administrator Designated** Minimum Security Clearance of Secret	**Secret**	Storage Locker
Secret LAN	**All Metal Room** **Cipher Lock** **Combination Lock** **Pad Lock** **Watch-Stander Checked**	**Minimum Security Clearance of Top Secret** **Lower clearance personnel logged and escorted**	**Top Secret**	Radio
Combat Information Center (CIC) Users	**All Metal Room** **Cipher Lock** **Combination Lock** **Pad Lock** **Watch-Stander Checked**	**Minimum Security Clearance of Secret** **Lower clearance personnel escorted** **Top Secret for designated areas when required for mission (Need-to-Know)**	**Secret with Top Secret increase when required for mission (Need-to-Know)**	CIC
Top Secret	**All Metal Room** **Cipher Lock**	**Minimum Top Secret (SCI)**	**Top Secret (SCI) (Need-to-Know)**	Sensitive Equipment Space

	Physical Security	Personnel Security	Space Rating	Space Location
LAN	**Combination Lock Pad Lock Camera Watch-Stander Checked**	**Lower clearance personnel logged and escorted (Need-to-Know)**		(SES)

Table 17. Current Shipboard Space and Personnel Security

Cryptographic threats and objectives have been included in the NP Protection Profile to address the future use of smart cards in conjunction with user login, authentication, and verification. With the NP located on the high side it is assumed that all physical security measures have been to taken to adequately secure the high side space.

The threats were evaluated based on the above environments in which the NP would be incorporated. The threats were tailored from the MGHREPP. The NP Security Target threats were also reviewed as to applicability to the NP Protection Profile.

Section Four's identification of objectives is tailored from the MGHREPP. The NP Security Target objectives were also reviewed as to applicability to the NP Protection Profile. The objectives chosen best fit the NP's threats and intended environments.

Section Five's identification of Security Functional Requirements (SFRs) are tailored from the MGHREPP. The NP Security Target SFRs also reviewed and applicable security functions are incorporated to best identify the SFRs required to address the threats and objectives previously identified. The desired security assurance level was identified to be an EAL5 to address the need to conduct covert channel analysis. Therefore, the security assurance requirements are exactly what the Common Criteria requires for an EAL5 Protection Profile. No tailoring on the security assurance requirements was performed to ensure the evaluation maintains the level of EAL5.

Section Six is derived from evaluating the threats, objectives and SFRs. All threats were supported by objectives and all objectives were supported by the SFRs. Tables were provided to give snap shots of the relationships between the threats and objectives and SFRs and objectives to give the developer, evaluator and other interested personnel an overview of their relationship. Table 18 below shows how an EAL 5

solution addresses three major threats in shipboard environments, and the causes for their concern.

Shipboard Threats	Security Components of Concern	EAL5 Solution
Administration	Confidentiality	Administrative/User Guidance
	Authentication	Administrative/User Guidance
	Availability	Auditing
	Network Integrity	Administrative Guidance Auditing
Covert Channel	Confidentiality	Independent Covert Channel Analysis Stringent Configuration Management Semi-Formal Development Methods Stringent Lifecycle Support Penetration Testing
	Accountability	Auditing
Identification/ Authentication	Confidentiality	Administrative/User Guidance Auditing DAC
	Authentication	DAC Administrative/User Guidance
	Availability	Administrative/User Guidance
	Data Integrity	Administrative/User Guidance
	Network Integrity	Administrative/User Guidance Auditing

Table 18. Threat and Security Component Solutions

As table 18 illustrates, the EAL5 certification does not provide all site-specific security functionality. The additional security functionality required to protect against the above threats are delineated in Table 17.

E. CONCLUSION

The NP Protection Profile is a working document and should be reviewed and updated on a regular basis. As the process of evaluating the threats and objectives is conducted, new vulnerabilities may arise or technologies may reduce or induce threats that may need to be addressed. Security evaluation is an ongoing process. The TOE and its documentation should be kept current to provide the best product and ensure the validation of the TOE still meets the C&A.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NETWORK PUMP CERTIFICATION AND ACCREDITATION

A. INTRODUCTION

The recently approved Directive 8500.1 [Ref. 6] has caused a fundamental shift in the approach used to certify and accredit information technology and information systems. In the past the DoN developed and employed government designed and developed products. The SYSCOMS was responsible for ensuring the security of a site information system. Under 8500.1, the users and war-fighters verify the protection of their own information systems. Commands now purchase COTS products or integrate GOTS products directly into their information systems. Because of the lack of training most site DAAs and ISMOs receive, together with their lack of IT experience, information systems that are easier to exploit. The lack of training and experience is a result of the Navy's stets ways of conducting business- systems installed by contractors, certified by contractors, and then accredited by contractors. The DAAs trusted the contractor's assessment of a site's security without understanding or knowing the actual process used to determine their recommendation. Today, with fewer system installations occurring and more component or application installations, accreditation has shifted to the local DAAs and ISMOs. This chapter will provide the site DAAs and ISMOs an outline of the process and responsibilities necessary to accomplish phases one through three of the certification and accreditation process for the NP.

B. PHASES ONE AND TWO

By definition, the NP is a guard, or cross-domain component, that limits the exchange of information between systems of different security levels [Ref. 3]. According to SPAWAR, the Navy's certification authority, a project manager must manage all guards [Ref. 19]. Because of this, the NP is a Program of Record (POR) component. This means that the first two phases of the C&A process are the responsibility of the project manager and will result in a type certification [Ref. 20].

The type certification allows for the segregation of the technical set of specified security requirements to the NP's particular design, in order that a comprehensive evaluation of the technical security requirements is performed once. The evaluation can

be reused at multiple sites with different DAAs. It is imperative that the Operational DAAs remember that the type certification evaluated the NP in a specific system against a specified set of requirements with assumptions about the operational environment.

Since this portion is controlled by a project manager, the key members of the C&A team will be a Developmental DAA (DDAA) who supports the program acquisition during the design and development of the NP and accredits it prior to deployment, a Certification Authority, a Certification Agent, and User Representatives. It is the PM's responsibility for overseeing the organization and management of the team to accomplish the required tasks and generate the type SSAA and any other support documentation [Ref. 9].

The goal of phase one is to acquire and develop the information necessary to understand the NP so that a detailed list of tasks can be established. Since the NP is not a legacy system the phase one activities of preparation, registration, and negotiation will start from scratch because the existing documentation upon which to base the SSAA does not exist.

The preparation activity must include looking at all available documents concerning the NP and applicable DoD and DoN information assurance and security instructions and policies. Since the NP is still under development by NRL there is no mission needs statement. The protection profile (Appendix C) identifies the user requirements. Other documents to be reviewed include the security target, architecture and design document, user manuals, operating procedures, configuration management documents, and the threat analysis.

The registration activity guides the C&A team to develop tasks for the evaluation of the NP necessary to address risk management. These tasks identify the security requirements and the level of effort necessary to complete the type certification. Once these are known, the DITSCAP will be tailored to prepare an effective plan that leads to the draft SSAA [Ref. 9].

In order to complete phase one for the NP, all parties involved will review the draft SSAA. The DDAA is responsible for verifying that all applicable information assurance and security requirements are included in the SSAA. SPAWAR is responsible

for conducting an evaluation of the technical security features of the NP based on the draft SSAA. The PM reviews the SSAA for completeness, while the user representative reviews it to ensure that the NP will still support their needs. After all reviews are completed and it is determined that the appropriate assurance is being applied, the phase one SSAA is approved and phase two begins. Appendix D contains a proposed draft SSAA for the NP.

Phase two involves ensuring compliance of the NP specifications, design, and code with the security requirements developed in phase one [Ref. 9]. These activities include preparing certification test plans and procedures, conducting a vulnerability evaluation, and performing the certification test and evaluation (CT&E). The CT&E is usually performed in a laboratory environment but could be performed at a selected field site [Ref. 21]. During phase two the SSAA may undergo refinement based upon things such as NP modifications, or changes in the user requirements. During this technical evaluation of the NP the certifying team will develop the Security Features Users Guide (SFUG) and the Trusted Facility Manual (TFM).

After all of the phase two activities are complete and the SSAA has been updated the results are reviewed and evaluated by SPAWAR who will then prepare a Certification Statement to advise the DDAA on whether to certify the NP for deployment. The DDAA makes the certification decision. In this thesis we assume that the NP obtains an Approval to Deploy, with a type SSAA. The type SSAA and the ISSO of the SSAA should clearly state the assumptions made about the operational environment.

C. PHASE THREE

Now that the NP has been granted a hypothetical Type Accreditation, the responsibility for completing the C&A process shifts to the Operational DAA; for the ship, this is the Commanding Officer. The NP should arrive with the required SSAA documenting the completion of phases one and two activities along with the type Accreditation, SFUG, TFM, and Users' Manual [Ref. 21]. It is possible, though, for the NP to be received from SPAWAR without a type SSAA and type Accreditation. According to reference 5239-13 Volume II the site should not accept the installation as complete if this happens.

During phase three, the site ISSM must perform the activities necessary to accredit the systems based upon the NP's integration into the local site. These activities include a review of the type SSAA, an evaluation of the integrated information system, certification of the system, and accreditation. During the review of the type SSAA, the ISSM must determine if there are any more stringent local security requirements, or unique site security risks, or deviations from the standard configuration or assumptions that change the Type Certification. If there are, then the ISSM must update the Requirements Tractability Matrix (RTM) in the Type SSAA and develop test procedures to validate those requirements.

With this completed, the ISSM can begin the certification and evaluation of the integrated system, which consists of eight tasks. The first four tasks:

1. Security Test and Evaluation (ST&E),
2. Penetration Testing,
3. TEMPEST and RED-BLACK Evaluation, and
4. COMSEC Compliance Evaluation,

are to assess the technical security features and assumptions of the configuration and implementation to ensure features affecting confidentiality, integrity, availability, and accountability have been implemented and performed properly. The baseline for these tests were established in phase two during CT&E by the type certification team. Because of this, the site team does not need to repeat the baseline tests. Instead they must only verify that the NP does not introduce additional risk to the site. This is done by examining any unique security issues to the site that were not accounted for in the CT&E.

If any tests are repeated then an analysis report must be included in the SSAA documenting the findings including an evaluation of vulnerabilities discovered during the evaluations, summary of the level of effort, tools used, and any recommendations. The last four certification evaluation tasks focus on the non-technical security features:

1. System Management Analysis,
2. Site Accreditation Survey,
3. Contingency Plan Evaluation, and
4. Risk Management Review.

These tests are designed to focus on Physical Security, Personnel Security, Procedural Security, Security Education, Training, and Awareness [Ref. 9]. Networks that the NP connects are required to run an automated security assessment tool to determine the security posture of the systems configuration [Ref. 21].

After the required tasks are completed, the results are evaluated by the ISSM for completeness and to determine if the activity is consistent with the SSSA. They are then added to the SSSA. If any problems are discovered during this process the PM must be informed. If a problem can be fixed the ISSM can then repeat the task and document the problem and the solution in the appropriate analysis report.

After completing the appropriate tasks for the evaluation of the integrated information system a residual risk assessment must be completed. This is a risk-based review of the task analysis reports to determine if the risk to confidentiality, integrity, availability, and accountability is being maintained at an acceptable level. The level of acceptable risk will vary from site to site depending upon DAA comfort levels.

From the risk assessment the ISSM can then prepare a local certification statement and accreditation recommendation for the DAA. This recommendation along with the finalized SSAA is presented to the DAA for review and decision on whether to accredit the system, not accredit the system, or grant an Interim Approval To Operate (IATO). When the system is accredited, the ISSM then incorporates the finalized type SSAA into the site SSAA, and the system enters phase four (post accreditation).

THIS PAGE INTENTIONALLY LEFT BLANK

V. NETWORK PUMP IMPLEMENTATION

A. CONCLUSION

This thesis project's overall goal was to determine the certification process required for the NP and the appropriate plan to implement this process. In answering this question there were four supporting questions that were answered first to determine a recommended path for certification of the NP.

The first supporting question involved a brief description of the NP and the required Protection Profile to incorporate into a component certification. Chapter I gives a general description of the NP's operation and also explains how it can benefit the Navy and fits in to the DoD goal of defense in depth. Then Chapter III discussed the methods to develop an EAL5 protection profile culminating in Appendix C, which is the protection profile for the NP.

The next question to answer was to determine the actual type certification and accreditation requirements from the appropriate DoD and DoN documents. Chapter IV gives discussions of the appropriate steps from the DITSCAP that are needed to type certify the NP for installation on board a ship. With this analysis the draft Type SSAA was created; this is Appendix D.

During the creation of the Protection Profile and draft Type SSAA common assumptions about the environment the NP was to be installed in were made to facilitate an effective analysis. These assumptions are described in Chapter III and in the ISSP of the draft Type SSAA. Once the NP achieves an EAL5 and Type certification it can be installed aboard ships. During the installation and certification these assumptions must be reviewed in detail to ensure that any inconsistencies between the assumed environment and actual installation environment do not degrade the overall site certification.

The final supporting question dealt with factors that will impede the successful implementation of the NP, and how they can be overcome. The largest factor that will impede successful implementation of the NP comes from the stove piped certification and accreditation processes used by NRL and SPAWAR.

The NP is currently undergoing a component-level certification at NRL, with no sponsorship from SPAWAR. NRL's goal is to certify the NP in the most generic environment available. This ensures that once component certification is complete NRL can try to sell the NP to as many DoD and other federal security agencies as possible. This certification is based strictly on the Common Criteria, using only a developer based Security Target which may not meet all defined user requirement as described in their Protection Profile. This thesis provides the PP needed by NRL to combine with their ST and CT&E to develop the ST&E to achieve the EAL5 certification. Figure 6 shows the current path NRL is using to obtain an EAL 5 Certification.

Figure 6. Present Certification Configuration

At the time of this writing SPAWAR and DoN have yet to decide upon the relevance of the NP to the fleet. Active fleet components have expressed a desire for a component with the NP capabilities. Until the leadership decides that the NP has a viable position in Navy systems the NP will continue to progress towards a generic component certification at NRL.

What this means is that if SPAWAR determines that the NP is applicable in the fleet, there will be significant delay before installation and application to certify the NP in Navy environments. SPAWAR will be required to establish a unique Program

Management Office. They will also be required to generate a protection profile to be used to implement the certification of the NP if a new greater EAL level is required. Once this is complete SPAWAR will need to enter into the DITSCAP process, starting with the production of a draft, Type SSAA, and create the CT&E, to complete phases one and two. Once this is completed a site specific ST&E must be prepared to certify and accredit the NP in a specific environment. Currently this all would be done through the efforts of NRL or in conjunction with NRL. Either path will result in a longer time delay for fleet deployment which early planning can avoid. Figure 7 shows the proposed path the NP will need to take if the NP is certified as an individual component.

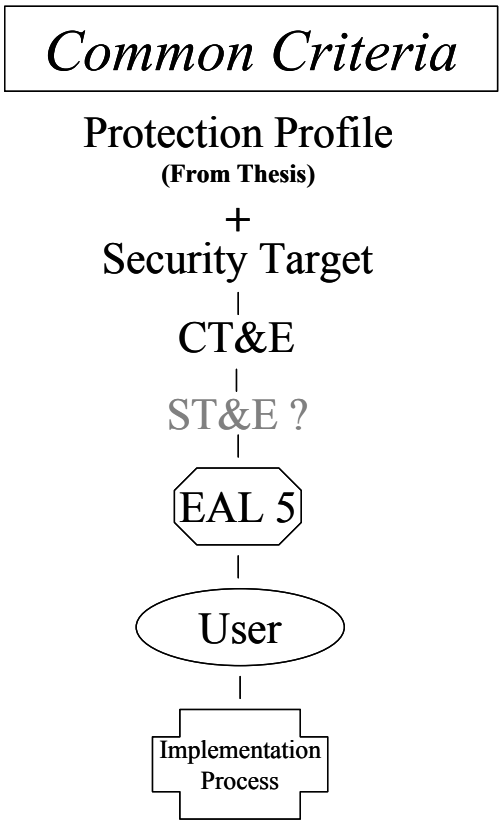

Figure 7. NRL Proposed Path

This thesis supports both NRL and SPAWAR efforts in evaluating the NRL NP. To NRL it provides the protection profile that is needed to accomplish the certification of the NP. To SPAWAR it provides a draft Type SSAA to start the DITSCAP process leading to the Type Certification and then to an accreditation for use by the fleet. Even

with these two much needed documents, the current stove piped work of NRL is not progressing towards fleet implementation.

In order to get this product to the fleet sooner it is recommended that SPAWAR establish a program with NRL to accomplish the Common Criteria requirements in conjunction with the phase one and two DITSCAP requirements. As discussed earlier, the program must be under the supervision of a program manager and it is recommended that the NP be placed under a pre-existing PM. This allows immediate funding to be provided for the certification of the NP.

Students in the Information Technology and Computer Science curriculums could accomplish the certification work at the Naval Postgraduate School. Their task would be to merge the ST and CT&E from NRL along with the PP and Type SSAA from this thesis to develop a common CT&E plan. This common CT&E plan could then be used in a simulated shipboard environment at NPS with appropriate ship specific security assumptions as needed to accomplish an EAL certification and complete a final Type SSAA. With this completed, SPAWAR could develop the appropriate ST&E for shipboard installation. By working together with NRL, SPAWAR, and NPS, the fleet can realize the benefits of the NP much sooner with a reduced overall cost. Figure 8 shows the recommend implementation path for the NP to be integrated into a shipboard system while obtaining an EAL 5 Certification.

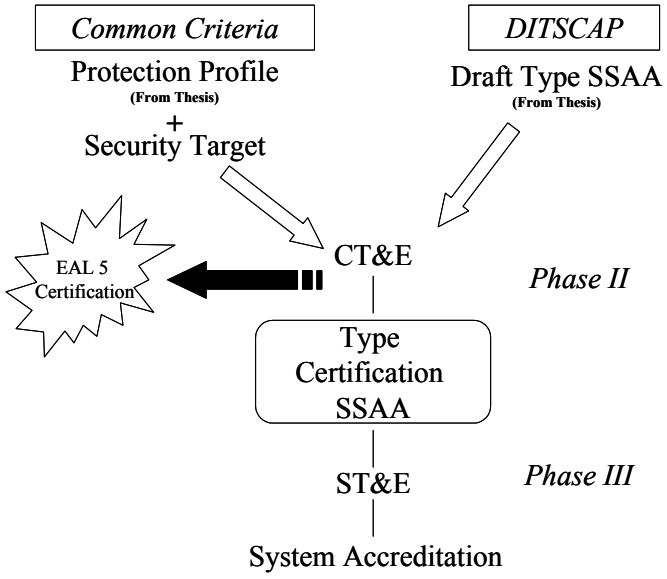

Figure 8. Proposed Implementation Path For System Integration

B. RECOMMEND FOLLOW-ON STUDIES

During the course of our research and discussion with individuals at the shipboard level, the concept of SSAAs and their management seemed unfamiliar. The Navy has policies for periodicity and system configuration changes that require a full or partial SSAA to be conducted. An effective tool for senior Navy leadership would be a baseline of site SSAAs across the entire fleet. This analysis would be for representative sites across DoN to determine the actual ability of the fleet to maintain the required accreditation. Part of this analysis work would also be to look at the training that is given to various people in the C&A process, for example the PCO and PXO school curriculums. This work could also be used to help develop more automated tools to assist those on the deck plates maintain their site's accreditation.

The area of IT community manpower and personnel, has the potential to identify weaknesses and recommend solutions to senior leadership. The Navy is unique in the fact that because we go to sea we must rotate people from sea to shore and back to sea. Other services do not have this problem because all of their billets are shore billets. The challenge that arises for the Navy from our sea and shore rotation is that when IT personnel go from a shore command to sea they are stepping backwards in technology. They also lose valuable training time in schools and professional conferences. These lost opportunities lead to stagnation that puts the Navy farther behind the technology curve. A study that identifies possible solutions to avoid this stagnation while keeping well trained operators in critical billets, could help the Navy move ahead in the IT world.

A final area of recommended study is in the area of IT system guidelines and procedures. Currently in DoD and DoN there is a plethora of high-level policy. This policy is good for senior-level technicians at a SYSCOM, but there is nothing in writing for the ship CO and his support staff of junior technicians to follow. For other technical areas of the ship there are operating manuals that give immediate actions for possible casualties or standard operating procedures from the SYSCOM. There is no such thing for the IT personnel. An analysis of this high level policy that is then turned into a set of actions or operating procedures for ships that may not have a large experienced IT division would be very beneficial.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. ACRONYMS

ACK	Acknowledgement
AIS	Automated Information System
BLP	Bell-La-Padula
CAPP	Controlled Access Protection Profile
C&A	Certification and Accreditation
CEM	Common Evaluation Methodology
CM	Configuration Management
CNO	Chief of Naval Operations
COTS	Commercial Off the Shelf
CRR	Certification Requirements Review
CSA	Communication Support Agreement
CT&E	Certification Test and Evaluation
CTCPEC	Canadian Criteria
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DCID	Defense Central Intelligence Directive
DDAA	Developmental Designated Approving Authority
DITSCAP	Defense Information Technology Security Certification and Accreditation
DoD	Department of Defense
DoDD	Department of Defense Directive
DoN	Department of the Navy
DTLS	Descriptive Top-Level Specification

EAL	Evaluation Assurance Level
ESI	Extremely Sensitive Information
FCD	Final Committee Draft
FIWC	Fleet Information Warfare Center
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
FTLS	Formal Top-Level Specification
GMT	General Military Training
GOTS	Government Off the Shelf
IA	Information Assurance
INFOCON	Information Condition
INFOSEC	Information Security
ISO	International Organization for Standards
ISSM	Information System Security Manager
ISSP	Information System Security Policy
IT	Information Technology
ITSEC	European Criteria
LAN	Local Area Network
LSPP	Labeled Security Protection Profile
MAC	Mandatory Access Control
MGHREPP	Mail Guard for High Robustness Environments Protection Profile
MLS	Multi-Level Secure
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding

NCIS	Naval Criminal Investigative Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and technology
NOC	Network Operations Center
NP	Network Pump
NRL	Navy Research Laboratory
NSA	National Security Agency
NSO	Network Security Officer
NSTISSC	National Security Telecommunications & Information Systems Security Committee
PDS	Protection Distribution System
PM	Program Manager
POR	Project of Record
RTM	Requirements Traceability Matrix
SFR	Security Functional Requirements
SFUG	Security Functional User Guide
SSAA	System Security Authorization Agreement
ST&E	Security Test & Evaluation
TCSEC	Trusted Computer Security
TFM	Trusted Facility Manual
TOE	Target of Evaluation

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. GLOSSARY

Clearances (The elements of the Glossary are paraphrased from [Ref. 7]):

Uncleared (U) - Personnel with no clearance or authorization. Permitted access to any information for which there are no specified controls, such as openly published information.

Unclassified Information (N) - Personnel who are authorized access to sensitive unclassified (e.g., For Official Use Only (FOUO)) information, either by an explicit official authorization or by an implicit authorization derived from official assignments or responsibilities.

Confidential Clearance (C) - Requires U.S. citizenship and typically some limited records checking. In some cases, a National Agency Check (NAC) is required (e.g., for U.S. citizens employed by colleges or universities).

Secret Clearance (S) - Typically requires a NAC, which consists of searching the Federal Bureau of Investigation fingerprint and investigative files and the Defense Central Index of Investigations. In some cases, further investigation is required.

Top Secret Clearance based on a current Background Investigation (TS(BI)) - Requires an investigation that consists of a NAC, personal contacts, record searches, and written inquiries. A BI typically includes an investigation extending back 5 years, often with a spot check investigation extending back 15 years.

Top Secret Clearance based on a current Special Background Investigation (TS(SBI)) - Requires an investigation that, in addition to the investigation for a BI, includes additional checks on the subject's immediate family (if foreign born) and spouse and neighborhood investigations to verify each of the subject's former residences in the United States where he resided six months or more. An SBI typically includes an investigation extending back 15 years.

One category (1C)1 - In addition to a TS(SBI) clearance, written authorization for access to one category of information is required. Authorizations are the access rights granted to a user by a responsible individual (e.g., security officer).

Multiple categories (MC) - In addition to TS(SBI) clearance, written authorization for access to multiple categories of information is required.

Data Sensitivities:

Unclassified (U)--Data that is not sensitive or classified: publicly releasable information within a computer system. Note that such data might still require discretionary access controls to protect it from accidental destruction.

Not Classified but Sensitive (N) - Unclassified but sensitive data. Much of this is FOUO data, which is that unclassified data that is exempt from release under the Freedom of Information Act. This includes data such as the following:

1. Manuals for DoD investigators or auditors.
2. These are actually authorizations rather than clearance levels, but they are included here to emphasize their importance.
3. Examination questions and answers used in determination of the qualification of candidates for employment or promotion.
4. Data that a statute specifically exempts from disclosure, such as Patent Secrecy data.
5. Data containing trade secrets or commercial or financial information.
6. Data containing internal advice or recommendations that reflect the decision-making process of an agency.
7. Data in personnel, medical, or other files that, if disclosed, would result in an invasion of personal privacy.
8. Investigative records. DoD Directive 5400.7 prohibits any material other than that cited in FOI Act exemptions from being considered or marked FOUO. One other form of unclassified sensitive data is that pertaining to unclassified technology with military application. This refers primarily to documents that are controlled under the Scientific and Technical Information Program or acquired under the Defense Technical Data Management Program. In addition to specific requirements for protection of particular forms of unclassified sensitive data, there are two general mandates. The first is Title 18, U.S. Code 1905, which makes it unlawful for any office or employee of the U.S. Government to disclose information of an official nature except as provided by law, including when such information is in the form of data handled by computer systems. Official data is data that is owned by, produced by or for, or is under the control of the DoD. The second is Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum Number I, which establishes requirements for Federal agencies to protect sensitive data.

Confidential (C) - Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Secret (S) - Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Top Secret (TS) - Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

One Category (1C) - Applied to Top Secret Special Intelligence information (e.g., Sensitive Compartmented Information (SCI) or operational information (e.g., Single Integrated Operational Plan/Extremely Sensitive Information (SIOP/ESI)) that requires special controls for restrictive handling. Access to such information requires authorization by the office responsible for the particular compartment.

Multiple Categories (MC) - Applied to Top Secret Special Intelligence or operational information that requires special controls for restrictive handling. This sensitivity level differs from the 1C level only in that there are multiple compartments involved. The number can vary from two to many, with corresponding increases in the risk involved.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Environment - The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. (See Open Security Environment and Closed Security Environment.)

Label – A piece of information that represents the security level of an object and that describes the sensitivity of the information in the object.

Malicious Logic - Hardware, software, or firmware that is intentionally included in a system for the purpose of causing loss or harm.

Mandatory Access Control - A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. NP PROTECTION PROFILE (PROPOSED)

1.0 PROTECTION PROFILE INTRODUCTION

1.1 Protection Profile Identification

Title: Network Pump Protection Profile
Sponsor: Naval Research Laboratory (NRL)
Authors: Ronald Rich and Jonathon Holmgren
Contributors: George Dinolt and Craig Rasmussen
CC Version: Common Criteria (CC) Version 2.1
Registration: <to be provided upon registration>
PP Version: Version 1.0, dated 01 November 2002
Keywords: Commercial-Off-The-Shelf (COTS), Naval Research Laboratories (NRL), Certification, Accreditation, Multi-Level Security, Secure Electronic Pump, Protection Profile, EAL5.

Note: The following outlines how the NP Protection Profile was derived: Section 1 is formatted from the CC, part 2; Section 2 is quoted directly from Section 2 of the NRL's Security Target; Section 3 is paraphrased from the DoD Mail Guard for High Robustness Environment, formatted from the CC, part 2 and tailored to meet the NRL NP security requirements; Section 4 is paraphrased from the DoD Mail Guard for High Robustness Environment, formatted from the CC, part 2 and tailored to meet the NRL NP security requirements; Section 5 is paraphrased from the DoD Mail Guard for High Robustness Environment, formatted from the CC, part 2 and tailored to meet the NRL NP security requirements; and Section 6 is paraphrased from the DoD Mail Guard for High Robustness Environment, formatted from the CC, part 2 and tailored to meet the NRL NP security requirements.

1.2 Protection Profile Overview

This Protection Profile (PP) specifies the information security requirements for the NP for High Robustness Environments. The NP specified in this PP sits between two protected network enclaves at different classification levels, controlling the flow of electronic messages sent between the two networks. The protection approach employs various processing, filtering, and data-blocking techniques in an attempt to prevent data exchange from the high side and the low side. Besides enforcing an information flow policy and providing services for confidentiality, assurance and integrity of messages, the NP provides identification and authentication, trusted path and audit capabilities and has been designed with a high degree of assurance.

The specific functional and assurance requirements are contained in Section 5 of this document.

1.3 Conventions

The notation, formatting, and conventions used in this Protection Profile are largely consistent with those used in version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP user.

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.

The **refinement** operation is used to add detail, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold tex**t.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized tex*t.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

The **security target writer** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security Target writer operations are indicated by the words {to be determined by the Security Target writer} in braces.

1.4 Terminology

In the CC, many terms are defined in Section 2.3 of Part 1. The following definitions are listed here to aid the users understanding of this PP.

Authorized Administrator - A role which human users may be associated with to administer the security parameters of the TOE. An Authorized Administrator is not subject to any access control requirements once authenticated to the TOE and is therefore trusted to not compromise the security policy enforced by the TOE. The Authorized Administrator is responsible for administering the TOE (i.e., operating system configuration) security parameters.

User Agent (UA) - A process that makes the services of the NP available to the user. A UA may be implemented as a computer program that provides utilities to create, send, receive, and perhaps archive messages.

1.5 PP Organization

Section 1, PP Introduction, provides document management and overview information necessary to identify the PP along with references to other related PPs.

Section 2, Target of Evaluation (TOE) Description, defines the TOE and establishes the context of the TOE by referencing generalized security requirements.

Section 3, TOE Security Environment (TSE), describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment.

Section 5, IT Security Requirements, defines the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the TOE.

Section 6, Rationale, provides rationale to demonstrate that the security objectives satisfy the threats and polices. This section also explains how the set of requirements are complete relative to the security objectives and presents a set of arguments that address dependency analysis and Strength of Function (SOF).

Expansion of acronyms is provided to facilitate comprehension of frequently used terms.

References are provided, as background material, for further investigation by interested users of the Protection Profile.

2.0 TOE DESCRIPTION

The general architecture in which the NP resides is shown in Figure 1. The NP supports communication connections from the Low LAN Interface to the High LAN Interface. These connections may support random traffic, e.g., e-mail, from the Low to High or more structured updates of High LAN databases, e.g., SQL updates that replicate Low LAN database updates to the High LAN. The NP supports a specialized protocol, called the *Pump Protoco*l, across the LAN interfaces for ease of re-use and maintenance. The NP operates compatibly with protocols from the TCP/IP suite. TCP/IP is usually described as supporting four layers (listed from lowest to highest): network access layer, internet layer, host-host transport layer, and application layer. The *Pump Protocol* is implemented at the application layer and uses the services provided by the transport layer.

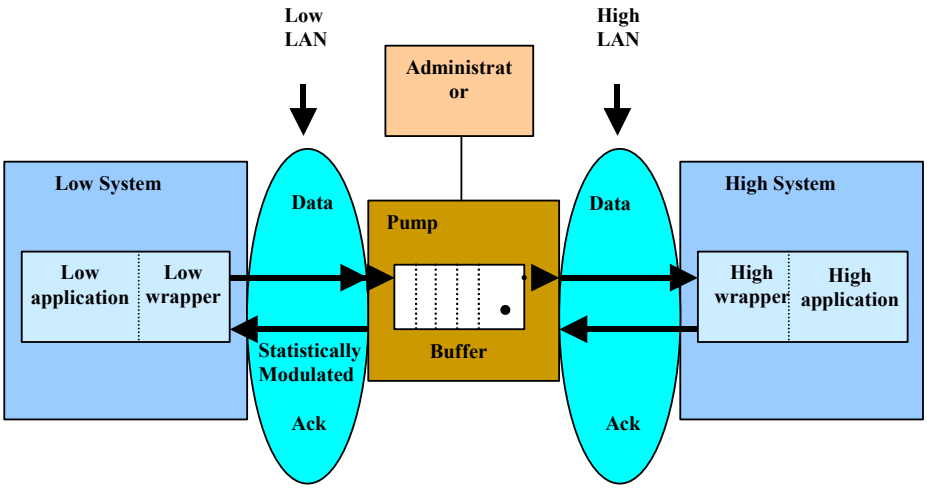

Figure 9. Network Pump

The ability to support a variety of applications is provided by components called *wrapper*s. These components run on the application systems in the Low and High enclaves that communicate with the NP over their respective LANs. Each application on the Low LAN that uses the NP communicates via an interface to a Low Wrapper, and, similarly, each application on the High LAN that receives information from the NP communicates via an interface to a High Wrapper. The wrappers are responsible for supporting the *Pump Protocol* on one side and the particular application protocol on the other. Different wrappers will support different applications; installing or modifying a wrapper is a change to the software configuration on the application system, but not to the NP. As shown in Figure 2, each wrapper is further divided into an application-dependent part, which can be tailored to support the particular set of objects, or calls the application expects to see, and a NP-dependent part, which is a library of routines that implement the *Pump Protocol*. These functions can be called as required by the application-dependent routines.

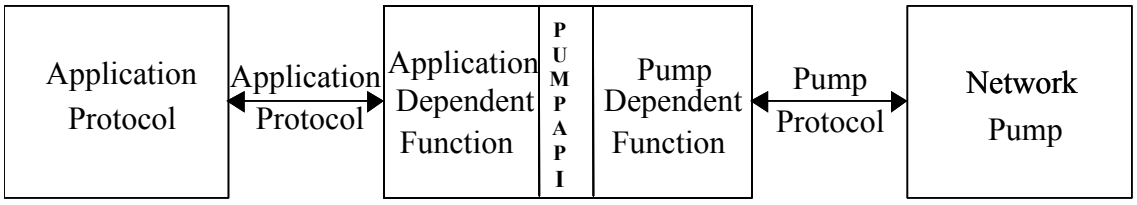

Figure 10. Structure of a Wrapper

The NP also provides the interface to an Administrator Terminal. The NP receives initial configuration and other control information across this interface and provides error and performance reports, if requested by the Administrator. The configuration information defines which users on the Low LAN are permitted to open connections (and thereby transmit messages) to which users on the High LAN.

2.1 Pump Protocol

The *Pump Protocol* is a special-purpose protocol implemented at the application layer that defines the communications at this level between the NP and the Low Wrapper and High Wrapper. The protocols used below the application layer (transport, internet, and network interface layers) must support communication across Ethernet LANs. The *Pump Protocol* is specified in terms of the messages it transmits. There are two classes of messages: Control Messages and Data Messages.

2.1.1 Control Messages

Control Messages support the creation and termination of connections. There are three types of control messages:

1. **Request Connection:** This message specifies the desired source and destination of the connection as an IP address and port number and specifies whether a recoverable or non-recoverable connection is desired. It is sent from the Low Wrapper to a well-known port on the NP.

2. **Connection Valid/Invali**d: This message is sent from the NP to a Low Wrapper in response to a Request Connection Message. If the message indicates a connection is invalid, it implies that the re-quested connection is not consistent with the Configuration Table or that the host is unavailable. If the requested connection is valid, the Low Wrapper is expected to listen for a Connection Granted message.

3. **Connection Granted**: This message is sent from the NP to a Low Wrapper following a Connection Valid message and indicates that the Low Wrapper can begin sending messages across the connection. The same message is also sent to the High Wrapper at the IP address and port specified in the connection request. It also provides communication parameters for the connection, including Connection ID, maximum message size, window size, and initial time out value. If the requested connection was re-coverable, and the previous connection between this pair of IP/port addresses was both recoverable and terminated abnormally within the past 24 hours, then the last message transmitted to High Wrapper across the previous connection is appended to this control message.

4. **Connection Exit**: This is a message sent by the NP to the High Wrapper and Low Wrapper to indicate that an existing connection is being terminated abnormally. It is to be sent when an Administrator requests that a connection be closed or when the NP detects an abnormal condition on a connection (e.g., High Wrapper ceases to accept messages, Low Wrapper ceases to send messages).

2.1.2 Data Messages

Data Messages support the flow of messages and acknowledgments across an existing connection and can also indicate the normal termination of a connection.

1. **Data Message (Low to High):** This protocol unit transmits a single, non-zero-length message from Low Wrapper to High Wrapper over the connection specified by a connection ID. The sender of a Data Message also provides a

Message ID, which can act as a sequence number. This Data Message is sent from the Low Wrapper to the NP and, subsequently, from the NP to the High Wrapper.

2. Acknowledgment (High to Low): This protocol unit acknowledges receipt by the receiver of a message, specified by a Message ID, over a connection, specified by a Connection ID. The NP will send a message of this type to the Low Wrapper after it successfully receives a Data Message from the Low Wrapper. The High Wrapper will send a message of this type to the NP whenever the High Wrapper successfully receives a Data Message from the NP.

3. Close Connection Message: This protocol unit is sent from the Low Wrapper to the NP, and subsequently from the NP to the High Wrapper to terminate a connection normally. It specifies a Connection ID.

2.2 Low Wrapper Functions

The Low Wrapper shall include an application-dependent part and Pump-dependent part. The Pump-dependent part of the Low Wrapper shall provide the following functions to the application-dependent part by invoking appropriate *Pump Protocol* operations:

1. Request Connection: The application specifies the desired destination and connection type.

2. Send Data: The application requests data to be sent over an existing connection.

3. Close Connection: The application signals that it has no more data to transmit.

The application-dependent part of the Low Wrapper will map application communication requirements into these functions as needed. The Pump-dependent part of the Low Wrapper may return information to the application-dependent part in response to each of these operations (for example, the connection request may be accepted or refused, and an acknowledgment may be returned after data are sent). Whether this information is conveyed by the application-dependent part back to the Low Application will depend on the Low Application's requirements.

2.3 High Wrapper Functions

The High Wrapper shall include a Pump-dependent part and an application-dependent part. The Pump-dependent part shall provide the following functions:

1. Receive Connection: This function returns the information provided by the Connection Granted message to enable initialization of data structures for a new connection.

2. Receive Message: This function returns the next message received from the NP for the connection that corresponds to this High Wrapper

3. **Send Acknowledgment:** This function transmits an Acknowledgment to be transmitted over the specified connection for a specified message.

The application-dependent part of the High Wrapper will map application communication requirements into these functions as needed. The Pump-dependent part of the High Wrapper may return information to the application-dependent part in response to each of these operations (for example, the NP may terminate a connection, causing an abnormal return from the requested operation). Whether this information is conveyed by the application-dependent part back to the High Application will depend on the High Application's requirements.

2.4 NP Functions

The fundamental function of the NP is to provide reliable transmission of information from the Low LAN to the High LAN while ensuring that High information cannot leak to the Low LAN. Confidentiality properties of the NP depend solely on the NP itself and not on the Wrappers. Wrapper function, including both application-dependent and Pump-dependent parts, is not confidentiality critical and can be altered or replaced without affecting system confidentiality. The confidentiality critical nature of NP function stems from the ability of a High user/process to control the timing of application-layer acknowledgements, as in the case of the Store and Forward Buffer when the buffer is full.

The NP ensures that communication over the LAN Interfaces conforms strictly to the *Pump Protoco*l; any other application-level traffic is logged as erroneous and discarded. The NP controls the timing of the acknowledgments sent across the Low LAN interface, and thus the covert timing channel, according to an algorithm provided in reference [1]. This algorithm bounds the capacity of the covert channel analytically as follows:

For each active connection, the NP maintains a separate variable that reflects the moving average of the time it takes the High Wrapper to accept messages from the High LAN Interface. The NP delays application-layer acknowledgments, which are sent in response to messages received from the Low Wrapper over this connection, randomly according to this moving average. At the application layer, messages received over this connection shall be acknowledged in the same order they are received. The only information flow from the High Wrapper to the Low Wrapper over a connection occurs through changes in the value of the moving average variable. This variable shall not be provided directly to the Low Wrapper but the Low Wrapper may estimate its value by observing the randomized delays between message transmission and receipt of acknowledgments.

The NP supports the functions of the *Pump Protocol* and Administrator Terminal requests as follows:

1. The NP responds to a Request Connection control message received from a Low Wrapper over the well-known port designated for this purpose by checking the request against the Configuration Table and, if the request is invalid, sending a

Connection Invalid message to the Low Wrapper. If the request is valid, a Connection Valid message is sent, and a Connection ID is allocated for this connection. The NP then constructs a Connection Granted message containing appropriate data for this connection. If the request is valid and recoverability is requested, the NP also check to see whether the previous connection between the requested sender and receiver was terminated abnormally. If so, it returns the last message successfully transmitted from Low to High on that connection to the Low Wrapper along with the Connection Valid message.

2. The NP responds to a Data Message from the Low Wrapper by checking that the specified connection is valid and that the message fits the connection's parameters. If the connection is valid, and there is space available in the NP Buffer, it stores the message in the NP Buffer, generates an acknowledgment delay based on the current value of the moving average for this connection and a random factor in accordance with the NP algorithms. After this delay elapses, the NP transmits the appropriate acknowledgment to the Low Wrapper. If space is not available in the NP Buffer, the NP will generate a timeout event for itself. If space becomes available in the NP Buffer prior to the occurrence of the timeout, the message will be handled as in the preceding paragraph, except that the random delay computed for the acknowledgment will be modified to take into account the time elapsed between the receipt of the message and its placement in the buffer. If the timeout occurs before space becomes available, the message is discarded without sending an acknowledgment, since the Low Wrapper, not having received an acknowledgment, will retransmit the message.

3. The NP responds to a Close Message from the Low Wrapper by forwarding that message to the High Wrapper freeing the data structures allocated to this connection, and recording the connection as having terminated normally.

4. The NP responds to an Acknowledgment received from the High Wrapper on a given connection by updating the value of the moving average for this connection appropriately and releasing all storage associated with this message. If this is a recoverable connection, the NP places the message corresponding to the acknowledgment in the "last successfully transmitted message" stable storage buffer for this connection prior to releasing the storage associated with this message.

5. The NP terminates any protocol operation that takes longer than the configured Network Inactivity Timeout Value to return a result. Following such a termination, the NP logs the fact of the termination and continues as if a Connection Exit request had been received from the Administrator Terminal to terminate this connection (see item 6 below).

6. The NP responds to a Connection Exit request from the Administrator Terminal by releasing temporary storage related to this connection, and, if it is a recoverable connection, marking the connection as abnormally terminated in a data structure that can be consulted the next time a connection between the same sender/receiver pair is requested.

7. The NP responds to a Load Configuration request received from the Administrator Terminal by immediately replacing the existing Configuration Table with the new Table. The Configuration table specifies general parameters such as window sizes, buffer sizes, time out periods, maximum connections per host, maximum connections per NP, the IP addresses and port numbers on the Low LAN from which the NP will accept connection requests and messages whether a particular IP address/port requires recoverable service, the IP addresses and port numbers on the High LAN to which the NP will deliver messages, and which of the Low addresses is authorized to send to which of the High ad-dresses.

8. The NP responds to a Retrieve Status request from the Administrator Terminal by returning the Configuration Table and the current contents of auditing and error-logging data structures. Status information includes error reports, such as the number of erroneous messages received and number of improper connections attempted since the last report, and performance data, such as the number of connections initiated, number of messages successfully transmitted per connection, average delay per message, and current moving average values.

9. The NP responds to a Renew Status request by both returning the current status information and reset-ting all counters and status indicators to their initial states, except for the system clock. The NP releases any messages saved from abnormally terminated conditions that are older than 24 hours in response to this request.

The NP maintains the following characteristics while implementing the functions of the *Pump Protoco*l:

Throughput: The NP supports a minimum average data throughput of 2 megabits per second, from Low Wrapper to High Wrapper. On average, the NP can receive data on a particular connection from the Low Wrapper at the same rate that the High Wrapper for that connection accepts data from the NP.

Recoverability: The NP provides recoverable service. That is, once Low Wrapper receives an application layer acknowledgment from the NP for a given message, it can safely assume that the message will be delivered to the High Wrapper by the NP, even if power failures or system crashes occur, either in the NP or the High Wrapper.

Accuracy and Validity: The NP and Wrappers do not degrade the accuracy or validity of any applications to which they are connected. Each message delivered to a High Application by the High Wrapper over a given connection corresponds exactly to a message received from the Low Application by the Low Wrapper.

Message and Acknowledgment Ordering: For each message received successfully by the NP from a Low Wrapper over a connection, the NP sends an acknowledgment message back to the Low Wrapper over the same connection, and the acknowledgments are sent in the same order that the messages are received. The NP delivers messages to the High Application by the High Wrapper in the same order they

are received from the Low Application by the Low Wrapper. (Note that these requirements apply at the application protocol layer and do not preclude the use of lower level protocols that may permit subdividing messages into packets, packet duplication, out-of-order delivery of packets, packet retransmission, etc., over both the High LAN and Low LAN interfaces).

Non-Duplication of Messages: The NP successfully delivers each data message successfully received from the Low Wrapper to the High Wrapper exactly once, for recoverable connections, and at most once, for non-recoverable connections.

Connection Independence: Abnormal behavior (such as message flooding or refusal to accept messages) on one connection will not affect the performance of other connections.

Connection Fairness: Connections that are behaving normally receive service on a fair basis.

Note: Section 2, TOE description, is taken directly from the NP Security Target [Ref. 8].

3.0 SECURITY ENVIRONMENT

DoD Directive 8500.1 Information Assurance requires that all information systems employ protection mechanisms according to the level of robustness required relative to the sensitivity of the data to be protected and the threat agents likely to be involved. TOEs compliant with this PP are intended to be used in a High Robustness Environment (HRE). High Robustness is defined in the 8500.1 as: "Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures [Ref. 5]."

The remainder of this section addresses assumptions about the security aspects of a compliant TOE environment, threats to TOE assets or to the TOE environment that must be countered, and organizational security policies that compliant TOEs must enforce.

3.1 Secure Usage Assumptions

A. NO_EVIL_PROGRAMS

There are no untrusted user programs on the TOE.

A. NO_EVIL_USERS

Authorized Administrators and NP users are non-hostile, appropriately trained and follow all administrator guidance. However, they are capable of error.

A. PHYSICAL_SECURITY

The TOE will reside in a physically secure environment on the high side.

The physically secure environment will be under controlled access where personnel will have authorization into the command, be on a controlled access list, or be escorted by designated authorized personnel.

A. TOE_ENTRY_POINT

Information cannot flow between the two enclaves without passing through the TOE.

3.2 Organizational Security Policies

P. MANDATORY_ACCESS_CONTROL

A mandatory access control policy based on hierarchical security levels and categories shall be enforced at the network level. Information shall not be allowed to flow from a higher security level to a lower security level or between non-comparable security levels. The only downward flow will be acknowledgements from high side, through the NP, to the low side.

3.3 Threats Addressed by the TOE

Note: The Threats are paraphrased from the MGHEPP and tailored for the NP.

T. ADMINISTRATION

A threat agent may make an error in the management of the TOE. Also, a threat agent may cause an error due to being given more privileges than required.

T. AUDIT_FULL

A threat agent may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust storage capacity, thus masking an attacker's actions.

T. AUDIT_UNDETECTED

A threat agent may cause auditable events to go undetected.

T. BRUTE_FORCE

A threat agent may repeatedly try to guess authentication data in order to launch an attack against the TOE.

T. BYPASS

A threat agent may attempt to bypass the security enforcing functions of the TOE.

T. COVERT_CHANNEL

A threat agent may use an entity not normally viewed as a data container (e.g., object) to transfer information from a container at one security level to a container at another security level.

T. DISCLOSURE

A threat agent may be able to gain access to information that is released in violation of the TOE security policy due to lack of confidentiality protection.

T. EXCESS_AUDIT

A threat agent may cause an Authorized Administrator to be unable to analyze audit data due to an excess volume of data being recorded.

T. MODERATE_ATTACK_POTENTIAL

A threat agent possessing high attack potential may attempt to bypass or tamper with the TOE security functions to gain access to the TOE or the assets it protects.

T. IDENTIFICATION_AUTHENTICATION

A threat agent may attempt to perform actions on the TOE without being held accountable for their actions.

T. MODIFY_DATA

A threat agent may attempt to modify or destroy security-critical TOE data or programs.

T. REPLAY

A threat agent may capture and replay valid identification and authentication information to disguise itself as an Authorized Administrator of the TOE.

T. SECURITY_LEVEL

A threat agent may cause data to be improperly protected due to the TOE's inability to correctly associate a security level with the data on export or import.

T. SYSTEM_FAILURE

A threat agent may cause the TOE to perform incorrectly resulting in a system failure.

3.4 Threats to the Environment

Threats to the physical environment could include fire or theft. However the likelihood of either in a shipboard (or controlled) environment is extremely low.

4.0 SECURITY OBJECTIVES

4.1 TOE Security Objectives

Note: The Objectives are paraphrased from the MGHEPP and tailored for the NP.

O. ACCOUNTABILITY

The TOE must be able to hold all users accountable for their actions. It must be possible to identify the user responsible for performing an action or sending a message. Security relevant events must be associated with the identity of the user. It must be possible to verify the sender of a message.

O. ADMIN_SUPPORT

The TOE must provide administrative tools to enable Authorized Administrators to effectively manage and maintain the TOE. The TOE must support these administrators in the performance of their duties and be designed to reduce the likelihood of administrative errors. The TOE must require a user to take an action before assuming an administrator role.

O. AUDIT

The TOE must provide a means to accurately detect and record security-relevant events in audit records. The TOE must detect and notify the Authorized Administrator when the audit log becomes full.

O. AUDIT_PROTECT

The TOE must protect the audit log from deletion and modification.

O. AUDIT_SELECT

The TOE must be able to change the selection of auditable events during normal operation.

O. AUTHENTICATION

The TOE must require that Authorized Administrators be authenticated (via a single-use authentication mechanism) before performing any TSF-mediated activities. Authentication of information passing through the TOE must be based on cryptographic mechanisms. The TOE must prevent brute force attacks by limiting the number of authentication attempts allowed in a session.

O. CONFIDENTIALITY

The TOE must be able to protect messages and other data from unauthorized disclosure.

O. COVERT_CHANNEL

The TOE must limit the number (i.e., capacity) and type of illicit information flows between security levels.

O. DATA_INTEGRITY

The TOE must be able to verify that messages and other data have not been modified.

O. DOMAIN_SEPARATION

The TOE must maintain its own domain for execution and ensure that it cannot be interfered with or tampered with by an untrusted subject.

O. IMPERSONATE

The TOE must provide a trusted path for Authorized Administrators to assure that they are communicating with the TOE when entering authentication information.

O. INFORMATION_FLOW

The TOE must not release information from a higher-level enclave to a lower level enclave or between non-comparable levels. Only communication from NP to low side will be an acknowledgement for received data.

O. NON-BYPASSABILITY

The TOE must ensure that a message cannot be released unless the configured filters are invoked and succeed.

O. RECOVERY

The TOE must be able to recover to a secure state in the event of system failure.

O. SELF_PROTECT

From its initial startup, the TOE must protect itself against attempts to modify, deactivate, or circumvent the TOE security functions.

O. SELF_TEST

A TOE must provide and execute self-tests during initial start-up, at the request of the security administrator, and during automated recovery to verify the integrity of its code and data structures.

O. SOF

The TOE must be able to meet strength of function equivalent to SOF-high.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

Note: The Objectives For the Environment are paraphrased from the MGHEPP and tailored for the NP.

OE. NO_EVIL_PROGRAMS

There are no untrusted user programs on the TOE.

OE. NO_EVIL_USERS

Authorized Administrators are non-hostile, appropriately trained and follow all administrator guidance. However, they are capable of error.

OE. PHYSICAL_SECURITY

The TOE will reside in a physically secure environment on the high side.

OE. TOE_ENTRY_POINT

Mail cannot flow between the two enclaves without passing through the TOE.

5.0 SECURITY REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the CC and assurance components from Part 3 of the CC.

5.1 TOE Security Functional Requirements

The applicable security functional requirements for the TOE are summarized in Table 19 below [Ref. 1, Part 2]. The functional components are presented in alphabetical order, by component name, in the CC.

Functional Components	
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FDP_ACC.1	Subset Object Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_ACF.3	Access Authorization and Denial
FDP_IFC.1	Subset information flow control
FDP_IFF.2	Hierarchical security attributes
FDP_IFF.3	Limited illicit information flows
FDP_RIP.2	Full residual information protection
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.4	Single-use authentication mechanisms
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_REV.1	Revocation
FMT_SMR.2	Restrictions on security roles
FMT_SMR.3	Assuming roles
FPT_AMT.1	Abstract machine testing
FPT_FLS.1	Failure with Preservation of Secure State
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_RCV.2	Automated recovery
FPT_RPL.1	Replay detection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.2	SFP domain separation
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TST.1	TSF testing
FTP_ITC.1	Inter-TSF trusted channel
FRU_RSA.1	Minimum and Maximum Quotas

Functional Components	
FTA_TSE.1	TOE Session Establishment
FTP_TRP.1	Trusted path

Table 19. Security Functional Requirements

The above SFRs are discussed in Section 5.1.1. The specific details will be filled in by Security Target writers upon further evaluation of the NP in a specific environment.

5.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 - The TSF shall be able to generate an audit record of the Audit Lo Events:

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the Functional components included in the PP/ST, are *source IP address, destination IP address, service, packet data, other data {to be determined by the Security Target writer}*.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 - The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 - The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [unsuccessful use of authentication mechanisms] known to indicate a potential security violation; and

b) Other events {to be determined by the Security Target writer}.

FAU_SEL.1 Selective audit

FAU_SEL.1.1 - The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) Event type; and

b) IP address, named sender, named recipient, type of attachment, and other attributes {to be determined by the Security Target writer}.

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 - The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 - The TSF shall take [measures to notify the Authorized Administrator] if the audit trail exceeds [90% storage capacity].

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 - The TSF shall *prevent auditable events, except those taken by the Authorized Administrator* and [shall limit the number of audit records lost] if the audit trail is full.

Application Note: The Security Target writer is expected to provide, as part of the "Security Requirements Rationale" section, an analysis of the maximum amount of audit data that can be expected to be lost in the event of audit storage failure, exhaustion, and/or attack.

5.1.2 User Data Protection (FDP)

FDP_ACC.1 - Subset Object Access Control

FDP_ACC.1.1 The TSF shall enforce the Admin Access Policy for all users accessing Admin Operations.

FDP_ACF.1 - Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the Admin Access Policy to objects based on the role of the user accessing Admin Operations.

FDP_ACF.1.2 The TSF shall ensure that only users authorized for the Administrator role can access Admin Operations on Admin Objects and that all new

connection requests immediately enforce any changes to the NP configuration that result from these operations.

FDP_ACF.3 – Access Authorization and Denial

FDP_ACF.3.1 The TSF shall ensure that the access control SF that enforces the Admin Access Policy shall explicitly authorize access to Admin Operations for users authorized for the Administrator role.

FDP_ACF.3.2 The TSF shall ensure that the access control SF that enforces the Admin Access Policy shall explicitly deny access to Admin Operations for users not authorized for the Administrator role.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [Mandatory Access Control SFP] on

[Operations: Information flow from one network enclave to another network enclave].

Application Note: With respect to the Mandatory Access Control SFP, a flow is equivalent to a write to the destination network enclave.

FDP_IFF.2 Hierarchical security attributes

FDP_IFF.2.1 - The TSF shall enforce the [Mandatory Access Control SFP] based on the following types of subject and information security attributes: [

a) Subject Security Attributes: Security level of the source network enclave; and
b) Information Security Attributes:
Security level of the destination network enclave;
Sender status (restricted or unrestricted);
Recipient status (restricted or unrestricted);
Other security attributes {to be determined by the Security Target writer}].

FDP_IFF.2.2 - The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [A subject can read an object if the hierarchical classification in the subject's security level is greater than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the subject's security level include all the non-hierarchical categories in the objects security level. A subject can write an object only if the hierarchical classification in the subject's security level is less than or equal to the hierarchical classification in the object's security level and the non-hierarchical categories in the Subject's security levels are included in the non-hierarchical categories in the object's security level].

FDP_IFF.2.3 - The TSF shall enforce the [Additional Information Flow Control rule as follows: The NP shall be configured to allow messages to flow from one network enclave at one security level to another network enclave at a potentially different security level (i.e., one for each source to destination network pair). The NP shall be configured to ensure that messages shall only flow between network enclaves under conditions that support the enforcement of the Mandatory Access Control SFP].

FDP_IFF.2.4 - The TSF shall provide the following [configurable security filters to support the Additional Information Flow Control rule].

FDP_IFF.2.5 - The TSF shall explicitly authorize an information flow based on the following rules:

a) The TOE shall allow each received message whose destination identification data is destined for one or more authorized recipients to pass through the TOE. An authorized recipient is a recipient on a network connected to the TOE who is allowed to receive messages through the TOE. An authorized recipient shall be a direct addressee (i.e., identified as a "TO:" recipient) or a courtesy copy addressee (i.e., identified as a "CC:" recipient).

b) The TOE shall allow each received message whose source identification data is from an authorized host to pass through the TOE.

c) The TOE shall allow each received message whose destination identification data is from an authorized host to pass through the TOE.

d) Additional Mandatory Access Control SFP rules {to be determined by the Security Target writer}].

FDP_IFF.2.6 - The TSF shall explicitly deny an information flow based on the protocols not supported by the TOE shall not be allowed to traverse the TOE.

FDP_IFF.2.7 - The TSF shall enforce the following relationships for any two valid information flow control security attributes:

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and

b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and

c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

FDP_IFF.3 Limited illicit information flows

FDP_IFF.3.1 - The TSF shall enforce the [Mandatory Access Control SFP] to limit the capacity of [network-accessible illicit information flows] to a [ST assignment: maximum capacity].

Application Note: The ST author is expected to define the maximum capacity of all network-accessible illicit information flows and to provide an argument as to why each capacity is appropriate.

FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

5.1.4 Identification And Authentication (FIA)

TOE security functions implemented by a probabilistic or permutation mechanism (e.g., password function) are required (at EAL2 and higher) to include a Strength of Function (SOF) claim. The single-use authentication mechanism must demonstrate SOF-high. SOF-high is defined in Part 1 of the CC to be ideal level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately, planned, or organized breach of TOE security by attackers possessing a high attack potential.

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 - The TSF shall detect when [a settable, non-zero number {to be determined by the Security Target writer(s)}] of unsuccessful authentication attempts occur related to [user authentication].

FIA_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the identified user from successfully authenticating itself to the TOE until an action is taken by the Authorized Administrator].

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users: [identity, role associations, security clearance, and any other user security attributes {to be determined by the Security Target writer(s)}].

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 - The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 - The TSF shall prevent reuse of authentication data related to [one-time passwords, digital certificates or biometrics].

FIA_UID.2 User identification before any action

FIA_UID.2.1 - The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security Management (FMT)

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 - The TSF shall restrict the ability to *enable, disable, determine and modify the behavior of* the functions:

a) Security monitoring rules;
b) Actions to be taken in case of imminent audit storage failure;
c) Actions to be taken in the event of authentication failure;
d) Group of users assigned to a security role and their assigned functions;
e) Conditions under which abstract machine testing and self-test occurs;
f) Types of service failures handled;
g) List and actions for which replay is detected; and
h) Actions requiring trusted path;
to [an Authorized Administrator].

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 - The TSF shall enforce the Admin Policy to restrict to users authorized for the Administrator role the ability to modify the roles of the users.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 - The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 - The TSF shall enforce the [Mandatory Access Control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 - The TSF shall allow the *Authorized Administrator* to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 - The TSF shall restrict the ability to read or modify the Admin Objects to users authorized for the administrator role.

FMT_REV.1 - Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke role permissions associated with users within the TSC to users authorized for the Administrator role.

FMT_REV.1.2 The TSF shall enforce revocation of a user's Administrator role on the next authentication of that user.

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 - The TSF shall maintain the roles: [Authorized Administrator and other roles {to be determined by the Security Target writer(s)}].

FMT_SMR.2.2 - The TSF shall be able to associate users with roles.

FMT_SMR.2.3 - The TSF shall ensure that the conditions [Authorized Administrator functions are appropriately separated and a user authorized to exercise functions in one role can be prevented from exercising functions simultaneously in another role] are satisfied.

FMT_SMR.3 Assuming roles

FMT_SMR.3.1 - The TSF shall require an explicit request to assume the following roles:

[Authorized Administrator and other roles {to be determined by the Security Target writer(s)}].

5.1.6 Protection of the TOE Security Functions (FPT)

FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 - The TSF shall run a suite of tests *during initial start-up, at the request of an authorized Administrator, and during automated recovery* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1 The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.

FPT_FLS.1 – Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the system, a connection or the power fails.

FPT_RCV.2 Automated recovery

FPT_RCV.2.1 - When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 - For [system failure and other failures {to be determined by the Security Target writer(s)}], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RPL.1 Replay detection

FPT_RPL.1.1 - The TSF shall detect replay for the following entities: [Authorized Administrator authentication].

FPT_RPL.1.2 - The TSF shall perform [ignore the attempted replay operation and generate an audit record] when replay is detected.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.2 SFP domain separation

FPT_SEP.2.1 - The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.2.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_SEP.2.3 - The TSF shall maintain the part of the TSF related to [Mandatory Access Control SFP] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 - The TSF shall be able to provide reliable time stamps for its own use.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 - The TSF shall provide the capability to consistently interpret [security labels] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 - The TSF shall use [the following rule to interpret security labels: if the security label of the message does not match the label in the classification field, the TOE shall not release the message] when interpreting the TSF data from another trusted IT product.

FPT_TST.1 TSF testing

FPT_TST.1.1 - The TSF shall run a suite of self-tests *during initial start-up, at the request of the authorized Administrator,* and [during automated recovery] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 - The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 - The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.1.7 Resource Utilization

FRU_RSA.2 – Minimum and Maximum Quotas

FRU_RSA.2.1 The TSF shall enforce quotas limiting the maximum quantity of the currently allocated connection resources that individual users can use over a specified period of time.

FRU_RSA.2.2 The TSF shall ensure the provision of minimum quantity of the currently allocated connection resources that individual users can use over a specified period of time.

5.1.8 TOE Access

FTA_TSE.1 – TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session (connection) establishment based on a user's location and/or port of access.

5.1.9 Trusted Path (FTP)

FTP_TRP.1 Trusted path

FTP_TRP.1.1 - The TSF shall provide a communication path between itself and *local* Authorized Administrator(s) that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 - The TSF shall permit *local Authorized Administrator(s)* to initiate communication via the trusted path.

FTP_TRP.1.3 - The TSF shall require the use of the trusted path for *initial Authorized Administrator(s) authentication* and [other services {to be determined by the Security Target writer}].

5.2 Security Requirements for the Environment

a) All physical security precautions will be taken for the proper level on the high side in which the NP will reside.

b) All personnel having access to the NP will hold the appropriate clearance commensurate to level of data being processed.

5.3 TOE Security Assurance Requirements

The TOE assurance requirements are EAL5 as shown in Table 20.

Assurance Class	**Assurance Components**	
Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.3	Development tools CM coverage
Delivery and Operations	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.3	Semiformal functional specification
	ADV_HLD.3	Semiformal high-level explanation
	ADV_IMP.2	Implementation of the TSF
	ADV_INT.1	Modularity
	ADV_LLD.2	Descriptive low-level design
	ADV_RCR.2	Semiformal correspondence demonstration
	ADV_SPM.3	Formal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_LCD.2	Standardized life-cycle model
	ALC_TAT.2	Compliance with implementation standards
Tests	ATE_COV.2.	Analysis of coverage
	ATE_DPT.2	Testing: low-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Assurance Class	Assurance Components	
Vulnerability Assessment	AVA_CCA.1	Covert channel analysis
	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation Vulnerability assessment
	AVA_VLA.3	Moderately resistant

Table 20. Security Assurance Requirements

5.3.1 Configuration Management (ACM)

ACM_AUT.1 Partial CM automation

Developer action elements:

ACM_AUT.1.1D - The developer shall use a CM system.

ACM_AUT.1.2D - The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C - The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C - The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C - The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C - The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_CAP.4 Generation support and acceptance procedures

Developer action elements:

ACM_CAP.4.1D - The developer shall provide a reference for the TOE.

ACM_CAP.4.2D - The developer shall use a CM system.

ACM_CAP.4.3D - The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C - The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C - The TOE shall be labeled with its reference.

ACM_CAP.4.3C - The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C - The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C - The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C - The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C - The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C - The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C - The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C - The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C - The CM system shall support the generation of the TOE.

ACM_CAP.4.12C - The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.3 Development tools CM coverage

Developer action elements:

ACM_SCP.3.1D - The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.3.1C - The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, security flaws and development tools and related information.

ACM_SCP.3.2C - The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.3.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

ADO_DEL.2 Detection of modification

Developer action elements:

ADO_DEL.2.1D - The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D - The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C - The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C - The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C - The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

ADO_DEL.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation generation and start-up procedures

Developer action elements:

ADO_IGS.1.1D - The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C - The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E - The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

ADV_FSP.3 Semiformal functional specification

Developer action elements:

ADV_FSP.3.1D - The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.3.1C - The functional specification shall describe the TSF and its external interfaces using a semiformal style, supported by informal, explanatory text where appropriate.

ADV_FSP.3.2C - The functional specification shall be internally consistent.

ADV_FSP.3.3C - The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.3.4C - The functional specification shall completely represent the TSF.

ADV_FSP.3.5C - The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

ADV_FSP.3.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E -The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.3 Semiformal high-level design

Developer action elements:

ADV_HLD.3.1D - The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.3.1C - The presentation of the high-level design shall be semiformal.

ADV_HLD.3.2C - The high-level design shall be internally consistent.

ADV_HLD.3.3C - The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.3.4C - The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.3.5C - The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.3.6C - The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.3.7C - The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.3.8C - The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing complete details of all effects, exceptions and error messages.

ADV_HLD.3.9C - The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.3.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.3.2E - The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.2 Implementation of the TSF

Developer action elements:

ADV_IMP.2.1D - The developer shall provide the implementation representation for the entire TSF.

Content and presentation of evidence elements:

ADV_IMP.2.1C - The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C - The implementation representation shall be internally consistent.

ADV_IMP.2.3C - The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements:

ADV_IMP.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.2.2E - The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

ADV_INT.1 Modularity

Developer action elements:

ADV_INT.1.1D - The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

ADV_INT.1.2D - The developer shall provide an architectural description.

Content and presentation of evidence elements:

ADV_INT.1.1C - The architectural description shall identify the modules of the TSF.

ADV_INT.1.2C - The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

ADV_INT.1.3C - The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

Evaluator action elements:

ADV_INT.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_INT.1.2E - The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

ADV_LLD.1 Descriptive low-level design

Developer action elements:

ADV_LLD.1.1D - The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C - The presentation of the low-level design shall be semiformal.

ADV_LLD.1.2C - The low-level design shall be internally consistent.

ADV_LLD.1.3C - The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C - The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C - The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C - The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C - The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C - The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C - The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing complete details of all effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C - The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

ADV_LLD.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E - The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.2 Semiformal correspondence demonstration

Developer action elements:

ADV_RCR.2.1D - The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.2.1C - For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.2.2C - For each adjacent pair of provided TSF representations, where portions of both representations are at least semi-formally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

Evaluator action elements:

ADV_RCR.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM.3 Formal TOE security policy model

Developer action elements:

ADV_SPM.3.1D - The developer shall provide a TSP model.

ADV_SPM.3.2D - The developer shall demonstrate or prove, as appropriate, correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.3.1C - The TSP model shall be Formal.

ADV_SPM.3.2C - The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.3.3C - The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.3.4C - The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.3.5C - Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.

ADV_SPM.3.6C – here the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be semiformal.

Evaluator action elements:

ADV_SPM.3.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D - The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C - The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C - The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C - The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C - The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C - The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C - The administrator guidance shall describe each type of security- relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C - The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C - The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D - The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C - The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C - The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C - The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C - The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C - The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C - The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life Cycle Support (ALC)

ALC_DVS.1 Sufficiency of security measures

Developer action elements:

ALC_DVS.1.1D - The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C - The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C - The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E - The evaluator shall confirm that the security measures are being applied.

ALC_LCD.2 Standardized life-cycle model

Developer action elements:

ALC_LCD.2.1D - The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.2.2D - The developer shall provide life-cycle definition documentation.

ALC_LCD.2.3D – The developer shall use a standardized life-cycle model to develop and maintain the TOE.

Content and presentation of evidence elements:

ALC_LCD.2.1C - The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.2.2C - The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.2.3C – The life-cycle definition documentation shall explain why the model was chosen.

ALC_LCD.2.4C – The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.

ALC_LCD.2.5C – The life-cycle definition documentation shall demonstrate compliance with the standardized life-cycle model.

Evaluator action elements:

ALC_LCD.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2 Compliance with implementation standards

Developer action elements:

ALC_TAT.2.1D - The developer shall identify the development tools being used for the TOE.

ALC_TAT.2.2D - The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.2.3D – The developer shall describe he implementation standards to be applied.

Content and presentation of evidence elements:

ALC_TAT.2.1C - All development tools used for implementation shall be well defined.

ALC_TAT.2.2C - The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.2.3C - The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.2.2E – The evaluator shall confirm that the implementation standards have been.

5.3.6 Testing (ATE)

ATE_COV.2 Analysis of coverage

Developer action elements:

ATE_COV.2.1D - The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C - The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C - The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.3C - The analysis of the test coverage shall rigorously demonstrate that all external interfaces of the TSF identified in the functional specification have been completely tested.

Evaluator action elements:

ATE_COV.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.2 Testing: low-level design

Developer action elements:

ATE_DPT.2.1D - The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.2.1C - The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.
Evaluator action elements:

ATE_DPT.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Ordered functional testing

Developer action elements:

ATE_FUN.1.1D - The developer shall test the TSF and document the results.

ATE_FUN.1.2D - The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C - The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C - The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C - The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C - The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C - The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D - The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C - The TOE shall be suitable for testing.

ATE_IND.2.2C - The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E - The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E - The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

AVA_CCA.1 Covert channel analysis

Developer action elements:

AVA_CCA.1.1D - The developer shall conduct a search for covert channels for each information flow control policy.

AVA_CCA.1.2D - The developer shall provide covert channel analysis documentation.

Content and presentation of evidence elements:

AVA_CCA.1.1C - The analysis documentation shall identify covert channels and estimate their capacity.

AVA_CCA.1.2C - The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

AVA_CCA.1.3C - The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.1.4C - The analysis documentation shall describe the method used for estimating channel capacity, based on worst-case scenarios.

AVA_CCA.1.5C - The analysis documentation shall describe the worst-case exploitation scenario for each identified covert channel.

Evaluator action elements:

AVA_CCA.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_CCA.1.2E - The evaluator shall confirm that the results of the covert channel analysis show that the TOE meets its functional requirements.

AVA_CCA.1.3E - The evaluator shall selectively validate the covert channel analysis through testing.

AVA_MSU.2 Analysis and testing for insecure states

Developer action elements:

AVA_MSU.2.1D - The developer shall provide guidance documentation.

AVA_MSU.2.2D - The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C - The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C - The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C - The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C - The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C - The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E - The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E - The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E - The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D - The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C - For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C - For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E - The evaluator shall confirm that the strength claims are correct.

AVA_VLA.3 Moderately resistant

Developer action elements:

AVA_VLA.3.1D - The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.3.2D - The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.3.1C - The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.2C - The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.2.3C - The evidence shall show that the search for vulnerabilities is systematic.

Evaluator action elements:

AVA_VLA.3.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.3.2E - The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.3.3E - The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.3.4E - The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.3.5E - The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

6.0 RATIONALE

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined in Section 4 and Section 5, respectively. Additionally, this section describes the rationale for the Assurance Requirements; rationale for not satisfying all of the dependencies; and the rationale for the Strength of Function (SOF).

Table 21 illustrates the mapping from Security Objectives to Threats and Policies. Table 22 illustrates the mapping of the Functional Requirements to Security Objectives.

6.1 Rationale for TOE Security Objectives

O. ACCOUNTABILITY

This security objective is necessary to counter the threats: T.IDENTIFICATION_AUTHENTICATION because it requires that users be properly identified and held accountable for their actions (including sending messages) or when they use security functions. This security objective also necessitates that security-related events be associated with the identity of the user for purposes of auditing.

O. ADMIN_SUPPORT

This security objective is necessary to counter the threats: T.ADMINISTRATION and T.EXCESS_AUDIT which have to do with ensuring that Authorized Administrators have the proper administrative tools to effectively perform their duties, maintain the secure operation of the TOE and decrease the likelihood of administrative errors. This security objective necessitate that an action, required by the TOE, be taken prior to granting the, role of Authorized Administrator.

O. AUDIT

This security objective is necessary to counter the threats: T.AUDIT_FULL and T.AUDIT_UNDETECTED. It ensures that security-relevant events are detected and completely and accurately recorded. This security objective also ensures that the TOE detects when the audit log is approaching its capacity, and notifies the Authorized Administrator.

O. AUDIT_PROTECT

This security objective is necessary to counter the threats: T.AUDIT_FULL and T.EXCESS_AUDIT. It ensures that the audit log is protected from deletion and modification.

O. AUDIT_SELECT

This security objective is necessary to counter the threat: T.EXCESS_AUDIT because it ensures that the Authorized Administrator is able to change the selection of auditable events during normal TOE operation.

O. AUTHENTICATION

This security objective is necessary to counter the threats: T.BRUTE_FORCE and T.IDENTIFICATION_AUTHENTICATION because it requires that users are uniquely identified via a single-use authentication mechanism and only granted a limited number of authentication attempts prior to accessing the TOE.

O. CONFIDENTIALITY

This security objective is necessary to counter the threats and policy: T.DISCLOSURE, T.INCORRECT_LEVEL because it requires that the TOE utilizes encryption and employs cryptography of adequate strength to protect messages and data from unauthorized disclosure.

O. COVERT_CHANNEL

This security objective is necessary to counter the threat: T.COVERT_CHANNEL because it requires that the type and capacity of elicit information flows are limited.

O. DATA_INTEGRITY

This security objective is necessary to counter the threat: T.MODIFY_DATA because it requires that messages and security-related data are protected from unauthorized modification.

O. DOMAIN_SEPARATION

This security objective is necessary to counter the threat: T.MODIFY_DATA because it ensures that the TOE is resistant to interference, modification or destruction by unauthorized external sources and that its domain is strictly maintained for execution.

O. IMPERSONATE

This security objective is necessary to counter the threat: T.REPLAY. It requires that a trusted path be established between the user and the TOE when entering authentication information. Additionally, it ensures that all digital signatures are validated.

O. INFORMATION_FLOW

This security objective is necessary to counter the threats and policy: T.INCORRECT_LEVEL, T.SECURITY_LEVEL, and P.MANDATORY_ACCESS_CONTROL because it ensures that information residing on the TOE is not released from a higher-level enclave to an enclave containing a lower security level or between non-comparable security levels. This security objective also ensures that the TOE is able to correctly associate a security level with data upon import or export.

O. NON-BYPASSABILITY

This security objective is necessary to counter the threats: T.BYPASS, T.DISCLOSURE and T.MODERATE_ATTACK_POTENTIAL because it requires that

the TOE is always invoked and that messages are not releasable until the security enforcement functions are invoked and successful.

O RECOVERY

This security objective is necessary to counter the threat: T.SYSTEM_FAILURE because it requires that the TOE automatically recovers to a secure state upon the event of a system failure or discontinuity of operation.

O. SELF_PROTECT

This security objective is necessary to counter the threats: T.BYPASS, T.MODIFY_DATA, T.SYSTEM_FAILURE, and T.MODERATE_ATTACK_POTENTIAL because it requires that the TOE protect itself from attempts to bypass, modify, destroy or tamper with TOE security-critical TOE data or programs.

O. SELF_TEST

This security objective is necessary to counter the threats: T.MODIFY_DATA and T.SYSTEM_FAILURE because it requires the TOE to execute a suite of self tests during initial startup, upon request by the Authorized Administrator and during automated recovery (i.e., in the event of a system failure) to ensure the integrity of the TOE code and its data structures.

O. SOF

This security objective is necessary to counter the threat:

T.MODERATE_ATTACK_POTENTIAL because it requires that the TOE is resistant to penetration attacks performed by a threat agent possessing a high attack potential.

	O.ACCOUNTABILITY	O.ADMIN_SUPPORT	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_SELECT	O.AUTHENTICATION	O.CONFIDENTIALITY	O.COVERT_CHANNEL	O.DATA_INTEGRITY	O.DOMAIN_SEPARATION	O.IMPERSONATE	O.INFORMATION_FLOW	O.NON-BYPASSIBILITY	O.RECOVERY	O.ROLE_SEPARATION	O.SELF_PROTECT	O.SELF_TEST	O.SOF
T.ADDRESS_SPOOFING	X					X												
T.ADMINISTRATION		X																
T.AUDIT _FULL			X	X														
T.AUDIT_UNDETECTED			X															

	O.ACCOUNTABILITY	O.ADMIN_SUPPORT	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_SELECT	O.AUTHENTICATION	O.CONFIDENTIALITY	O.COVERT_CHANNEL	O.DATA_INTEGRITY	O.DOMAIN_SEPARATION	O.IMPERSONATE	O.INFORMATION_FLOW	O.NON-BYPASSIBILITY	O.RECOVERY	O.ROLE_SEPARATION	O.SELF_PROTECT	O.SELF_TEST	O.SOF
T.BRUTE_FORCE						X												
T.BYPASS													X			X		
T.COVERT_CHANNEL								X										
T.DISCLOSURE							X						X					
T.EXCESS_AUDIT		X		X	X													
T.MODERATE ATTACK_POTENTIAL													X			X		X
T.IDENTIFICATION_AUTHENTICATION	X					X									X			
T.INCORRECT_LEVEL							X					X						
T.MODIFY_DATA									X	X						X	X	
T.REPLAY											X							
T.SECURITY_LEVEL												X						
T.SYSTEM_FAILURE														X		X	X	
P.MANDATORY_ACCESS_CONTROL												X						

Table 21. Security Objectives to Threats/Policies Mapping

6.2 Rationale for Security Objectives/Requirements for the Environment

All of the security objectives for the environment are restatements of assumptions found in Section 3. Therefore, those security objectives for the environment trace to the assumptions trivially.

6.3 Rationale for Security Requirements

The functional and assurance requirements presented in this PP are mutually supportive and their combination meets the stated security objectives. The security requirements were derived according to the general model presented in Part 1 of the Common Criteria.

Table 21 demonstrates the relationship among the threats, policies and TOE security objectives. Table 22 demonstrates the mapping between the security requirements and the security objectives. Together these tables demonstrate the completeness and sufficiency of the security requirements.

FAU_GEN.1 Audit Data Generation

This component outlines the data that must be included in audit records and the events that must be audited. This component traces back to and aids in meeting the following objective: O.AUDIT.

FAU_SAA.1 Potential Violation Analysis

This component ensures that repeated failed attempts to authenticate are monitored and alarmed if a threshold is reached. This component traces back to and aids in meeting the following objective: O.AUTHENTICATION.

FAU_SEL.1 Selective Audit

This component ensures that the Authorized Administrator can dynamically change the set of events to be audited. This component traces back to and aids in meeting the following objectives: O.ADMIN_SUPPORT and O.AUDIT_SELECT.

FAU_STG.1 Protected Audit Trail Storage

This component ensures that the audit trail is always protected from tampering. This component traces back to and aids in meeting the following objective: O.AUDIT_PROTECT.

FAU_STG.3 Action in Case of Possible Audit Data Loss

This component ensures that the Authorized Administrator is notified when the audit trail is reaching its maximum capacity. This component traces back to and aids in meeting the following objective: O.AUDIT.

FAU_STG.4 Prevention of Audit Data Loss

This component ensures that the Authorized Administrator will be able to administer the audit trail should it become full. This component traces back to and aids in meeting the following objective: O.AUDIT.

FDP_ACC.1 Subset Object Access Control

This component ensures that the TOE EN enforces the Admin Access Policy for all users accessing the Admin Operations. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT and O.AUTHENTICATION.

FDP_ACF.1 Security Attribute Based Access Control

This component ensures that the TOE enforces the Admin Access Policy to objects based on the role of the user accessing Admin Operations. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT and O.AUTHENTICATION.

FDP_ACF.3 Access Authorization and Denial

This component ensures that the TOE enforces the processes that control the Admin Access policy to explicitly authorize access to Admin Operations for users authorized for the Administrator role. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT and O.AUTHENTICATION.

FDP_IFC.1 Subset Information Flow Control

This component identifies the entities involved in the Mandatory Access Control SFP. This component traces back to and aids in meeting the following objective: O.INFORMATION_FLOW.

FDP_IFF.2 Hierarchical Security Attributes

This component identifies the attributes of the subjects sending and receiving the information in the Mandatory Access Control SFP, as well as the attributes for the information itself. Then the operations identify under what conditions information is permitted to flow through the TOE. This component traces back to and aids in meeting the following objective: O.INFORMATION_FLOW.

FDP_IFF.3 Limited Illicit Information Flows

This component ensures that certain types of illicit information flows are limited to an acceptable capacity. This component traces back to and aids in meeting the following objective: O.COVERT_CHANNEL.

FDP_RIP.2 Subset Residual Information Protection

This component ensures that all electronic messages that have traversed through the TOE and all TOE internal data are inaccessible after deletion. This component traces back to and aids in meeting the following objective: O.CONFIDENTIALITY.

FIA_AFL.1 Authentication Failure Handling

This component ensures that human users who are not Authorized Administrators cannot endlessly attempt to authenticate. After some number of failures, defined by the Authorized Administrator, the user is unable from that point on to authenticate. This

component traces back to and aids in meeting the following objective: O.AUTHENTICATION.

FIA_ATD.1 User Attribute Definition

This component exists to provide attributes to distinguish Authorized Administrators from one another for accountability purposes and to associate the roles in FMT_SMR.2 with a user. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FIA_UAU.2 User Authentication Before Any Action

This component ensures that the users are authenticated before any action is allowed by the TSF. This component traces back to and aids in meeting the following objective: O.AUTHENTICATION.

FIA_UAU.4 Single-use Authentication Mechanisms

This component was chosen to ensure that Authorized Administrators use an authentication mechanism of adequate strength when authenticating to the TOE. This component traces back to and aids in meeting the following objective: O.AUTHENTICATION.

FIA_UID.2 User Identification Before Any Action

This component ensures that the users are identified to the TOE before anything occurs on behalf of the user. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FMT_MOF.1 (1) Management of Security Functions Behavior

This component ensures that the TOE restricts the ability to enable, disable, and modify the security filters to the Administrator. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT.

FMT_MOF.1 (2) Management of Security Functions Behavior

This component ensures that the TOE restricts the ability to modify the behavior of functions (e.g., security monitoring rules; actions to be taken in case of imminent audit storage failure; actions to be taken in the event of authentication failure; group of users assigned to a security role and their assigned functions; conditions under which abstract machine testing and self-test occurs; types of service failures handled; list and actions for which replay is detected; and actions requiring trusted path) to the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT.

FMT_MSA.1 Management of Security Attributes

This component ensures that the TSF restricts the ability to add, delete, and modify the\ security attributes that affect the Mandatory Access Control SFP to only the Authorized Administrator. This component traces back to and aids in meeting the following objectives: O.ADMIN_SUPPORT.

FMT_MSA.2 Secure Security Attributes

This component ensures that appropriate values are assigned to the security attributes used in the Mandatory Access Control SFP. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT.

FMT_MSA.3 Static Attribute Initialization

This component ensures that there are restrictive default values implemented in the Mandatory Access Control SFP that the Authorized Administrator can change. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FMT_MTD.1 Management of TSF Data

This component ensures that the TSF restricts the ability to modify, delete, and assign user attributes (as defined in FIA_ATD.1.1), user identities (as defined in FIA_UID.2), authentication data (as defined in FIA_UAU.2) and timestamps (as defined in FPT_STM.1) to only the Authorized Administrator. This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT.

FMT_REV.1 Revocation

This component ensures that the TOE restricts the ability to revoke role permissions associated with users with the TSC to users authorized for the Administrator role. This component traces back to and aids in meeting the following objective: O.ACCOUNTABILITY.

FMT_SMR.2 Restrictions on Security Roles

This component was chosen because each of the FMT components depends on the assignment of a user to the Authorized Administrator roles. This component traces back to and aids in meeting the following objective: O.ROLE_SEPARATION.

FMT_SMR.3 Assuming Roles

This component ensures that users must take an explicit action in order to assume a trusted role (i.e., Authorized Administrator). This component traces back to and aids in meeting the following objective: O.ADMIN_SUPPORT.

FPT_AMT.1 Underlying Abstract Machine Test

This component ensures that the security assumptions provided by the underlying abstract machine are tested during start-up. This component traces back to and aids in meeting the following objective: O.SELF_PROTECT.

FPT_FLS.1 Export of User Data without Security Attributes

This component ensures that the TOE preserves a secure state when the system, connection or the power fails. This component traces back to and aids in meeting the following objective: O.RECOVERY.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

This component ensures that the cryptographic keys and data transmitted between different parts of the TOE are not disclosed. This component traces back to and aids in meeting the following objective: O.CONFIDENTIALITY.

FPT_RCV.2 Automated Recovery

This component ensures that the TOE returns to a secure state in the event of system failure. This component traces back to and aids in meeting the following objective: O.RECOVERY.

FPT_RPL.1 Replay Detection

This component ensures that replay of authentication attempts are detected and disallowed. This component traces back to and aids in meeting the following objectives: O.AUTHENTICATION and O.IMPERSONATE.

FPT_RVM.1 Non-bypassability of the TSP

This component ensures that the TOE enforcement functions are always invoked from initial start-up. This component traces back to and aids in meeting the following objective: O.NON_BYPASSABILITY.

FPT_SEP.2 SFP Domain Separation

This component ensures that the TSF has a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.DOMAIN_SEPARATION.

FPT_STM.1 Reliable Time Stamps

This component was included because FAU_GEN.1 depends on having the date and time accurately recorded in the audit records. This component traces back to and aids in meeting the following objective: O.AUDIT..FPT_TDC.1 Inter-TSF TSF Data Consistency.

FPT_TST.1 TSF Testing

This component ensures the integrity of the operation of the TSF and to provide the Authorized Administrator a means to verify the integrity of the TSF code and data. This component traces back to and aids in meeting the following objective: O.SELF_TEST.

FRU_RSA.2 Minimum and Maximum Quotas

This component ensures that the TOE enforces the minimum and maximum quantities of the currently allocated connection resources that individual users can use over a specified period of time: O. COVERT_CHANNEL.

FTA_TSE.1 TOE Sessions Establishment

This component ensures that the TOE be able to deny session (connection) establishment based on a user's location and/or port of access. This component traces back to and aids in meeting the following objective: O.AUTHENTICATION

FTP_TRP.1 Trusted Path

This component ensures that a trusted path is available to users, giving them assurance that they are communicating with the TOE. This component traces back to and aids in meeting the following objective: O.IMPERSONATE.

	O.ACCOUNTABILITY	O.ADMIN_SUPPORT	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_SELECT	O.AUTHENTICATION	O.CONFIDENTIALITY	O.COVERT_CHANNEL	O.DATA_INTEGRITY	O.DOMAIN_SEPARATION	O.IMPERSONATE	O.INFORMATION_FLOW	O.NON-BYPASSIBILITY	O.RECOVERY	O.ROLE_SEPARATION	O.SELF_PROTECT	O.SELF_TEST
FAU_GEN.1			X														
FAU_SAA.1						X											
FAU_SEL.1		X															
FAU_STG.1				X													
FAU_STG.3			X														

	O.ACCOUNTABILITY	O.ADMIN_SUPPORT	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_SELECT	O.AUTHENTICATION	O.CONFIDENTIALITY	O.COVERT_CHANNEL	O.DATA_INTEGRITY	O.DOMAIN_SEPARATION	O.IMPERSONATE	O.INFORMATION_FLOW	O.NON-BYPASSIBILITY	O.RECOVERY	O.ROLE_SEPARATION	O.SELF_PROTECT	O.SELF_TEST
FAU_STG.4			X														
FDP_ACC.1		X				X											
FDP_ACF.1		X				X											
FDP_ACF.3		X				X											
FDP_IFC.1												X					
FDP_IFF.2												X					
FDP_IFF.3								X									
FDP_RIP.2							X										
FIA_AFL.1						X											
FIA_ATD.1	X																
FIA_UAU.2						X											
FIA_UAU.4						X											
FIA_UID.2	X																
FMT_MOF.1(1)		X															
FMT_MOF.1(2)		X															
FMT_MSA.1		X															
FMT_MSA.2		X															
FMT_MSA.3																X	
FMT_MTD.1		X															
FMT_REV.1	X																
FMT_SMR.2															X		
FMT_SMR.3		X															
FPT.AMT.1																X	
FPT_FLS.1														X			
FTP_ITC.1											X						
FPT_ITT.1							X										
FPT_RCV.2														X			
FPT_RPL.1						X					X						
FPT_RVM.1													X				
FPT_SEP.2										X							

	O.ACCOUNTABILITY	O.ADMIN_SUPPORT	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_SELECT	O.AUTHENTICATION	O.CONFIDENTIALITY	O.COVERT_CHANNEL	O.DATA_INTEGRITY	O.DOMAIN_SEPARATION	O.IMPERSONATE	O.INFORMATION_FLOW	O.NON-BYPASSIBILITY	O.RECOVERY	O.ROLE_SEPARATION	O.SELF_PROTECT	O.SELF_TEST
FPT_STM.1			X														
FPT_TDC.1																	
FPT_TST.1																	X
FRU_RSA.1								X									
FTA_TSE.1						X											
FTP_TRP.1											X						

Table 22. Functional Requirement to Security Objective Mapping

6.4 Rationale for Security Requirements

EAL5 Augmented was chosen to ensure a high-level of confidence in the security services used to protect information in NPs for high-robustness environments. The assurance selection was based on:

- Detailed conversations with the sponsor of the PP;
- Recommendations documented in the 8500.1 [Ref. 5];
- The required strength of function, SOF-high (Section 4.1)
- EAL requirements as specified in the *Preferred Assurance Components/Processes for Devices Protecting Classified Information* table (Reference Appendix C); and
- The postulated threat environment (Section 3.3).

The sponsor of this PP determined that certain security critical components of the NP require an EAL of 5 to ensure that the security engineering performed by the developer was based on rigorous development practices supported by specialized security engineering techniques, such as the use of a structured development process, development of environment controls, comprehensive configuration management and evidence of secure product delivery. The former guidance in the recently canceled 5200.28_STD policy was consulted and found to also support the chosen assurance level EAL 5.

In order to ensure the security of a high-assurance system, not only must vulnerability analysis be performed by the developer, but the NSA evaluator, through the use of independent functional testing, must search for vulnerabilities and demonstrate that they are highly resistant to penetration attackers with moderate attack potential (T.MODERATE_ATTACK_POTENTIAL). This level of testing is supported by requirements ATE_FUN.1, ATE_COV.2, and ATE_DPT.2.

The developer shall provide a mechanism to track and correct security flaws in the TOE that are discovered after initial delivery and installation. Additionally, the developer must provide for automatic distribution of security flaw reports and corrections to registered users that may be affected by the defect.

Lastly, the NSA evaluator must validate the developer's systematic covert channel analysis specified by requirement AVA_CCA.1, to confirm the non-existence of illicit information flows that may be exploited by threat agents possessing moderate attack potential.

6.5 Rationale for Not Satisfying All Dependencies

The FDP_IFC.1 dependency (i.e., FDP_IFF.1) is not included in this PP. This dependency is satisfied in this PP with the inclusion of FDP_IFF.2, which subsumes FDP_IFF.1.

The functional requirements FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1 and FMT_SMR.2 are dependent on the requirement FMT_SMR.1 (Security Roles). Since there are multiple roles within this PP (i.e., Authorized Administrators), it is required that the conditions or rules that control the relationship between these roles are specified. Therefore, functional requirement FMT_SMR.2 is included and is hierarchical to FMT_SMR.1. As such, the requirement FMT_SMR.1 is satisfied.

6.6 Rationale for Strength of Function Claim

Part 1 of the CC defines the "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function.

There are three strength of function levels defined in Part 1: SOF-basic, SOF-Medium and SOF-high. SOF-high is the strength of function level chosen for this PP. SOF-high states, the level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential. The rationale for choosing SOF-high was based on the TOE security objectives documented in Section 4 of this PP.

Additionally, the sponsor determined that the SOF-high level is vital to address the TOE security objectives that counter the threat T.MODERATE_ATTACK_POTENTIAL.

Consequently, the metrics (i.e., password and keys) chosen for inclusion in this PP were determined to be sufficient for SOF-high and would adequately protect data and messages in a High Robustness Environment.

ACRONYMS

CC Common Criteria for IT Security Evaluation
CM Configuration Management

DOD Department of Defense
DSA Directory Service Agent
DUA Directory User Agent

EAL Evaluation Assurance Level

HRE High Robustness Environment

IP Internet Protocol
IT Information Technology

MAC Mandatory Access Control
MTA Mail Transfer Agent
MTS Mail Transfer System

NSA National Security Agency

PP Protection Profile

SFP Security Function Policy
SOF Strength of Function

TOE Target of Evaluation
TSE TOE Security Environment
TSF TOE Security Functions
TSP TOE Security Policy

REFERENCES

[1] Brotzman, Robert L. (1985). *Computer Security Requirements: Guidance for Applying the TCSEC in Specific Environments*. Retrieved May 7, 2002, from http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-003-85.html.

[2] Naval Research Laboratory *Network Pump (NP) Security Target*, May 29, 2000.

[3] *Common Criteria for Information Technology Security Evaluatio*n, CCIB-99-031 through 033, Parts 1,2 and 3, Version 2.1, August 1999.

[4] *Digital Signature Standard (DS*S), FIPS PUB 186-2, January 2000.

[5] *Secure Hash Standar*d, FIPS Pub 180-1, April 1995.

[6] Draft Department of Defense Instruction, *IA Implementation 8500.bb*, June 7, 2001.

[7] 2001 *Information Assurance Technical Framewor*k, Version 3.0, September 2000.

[8] Department of Defense Directive No. 8500.*1, Information Assurance*, October 24, 2002.

[9] *Defense of Defense Mail Guard for High Robustness Environments Protection Profil*e, Version 0.1, September 30, 2001.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. DRAFT SSAA

The draft SSAA was created using the DITSCAP instruction, DITSCAP application manual, and appropriate certification templates provided from SPAWAR. Using these resources the template SSAA was tailored along with the ISSP to apply directly to the NP in a basic shipboard environment.

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

1.1 System Name and Identification

Center for High Assurance Computer Systems, Code 5540 Naval Research Laboratory (NRL), Washington, D.C. developed the NP for Space and Naval Warfare Systems Command, PD – 161, San Diego, CA acting as a Low to High network connection link.

The following shipboard environmental assumptions were made during the certification of the NP:

4 Windows NT 4.0 File Servers
2 MS Exchange Servers 5.0
2 Cisco 4000 Routers
2 MS Proxy Servers
7 Xylan ATM Switches
150 Windows NT 4.0 Workstations, UNCLAS
45 Windows NT 4.0 Workstations, CLASSIFIED

1.2 System Description

I. Purpose
   a. DoD levels of classification - information transfer from low to high.
      i. Cannot compromise high
      ii. How to send information
         1. Without compromising high
         2. Providing assurance
         3. Providing Non-repudiation
   b. The NP is a general-purpose device to provide reliable, secure communications between systems in two enclaves, one operating at low and the other at high. The NP connects two or more LANs operating at different security levels.

II. Capability Desired
   a. Allow trusted users to send information from low to high.
   b. Ensure high users can access all required low information on high.

III. System Architecture

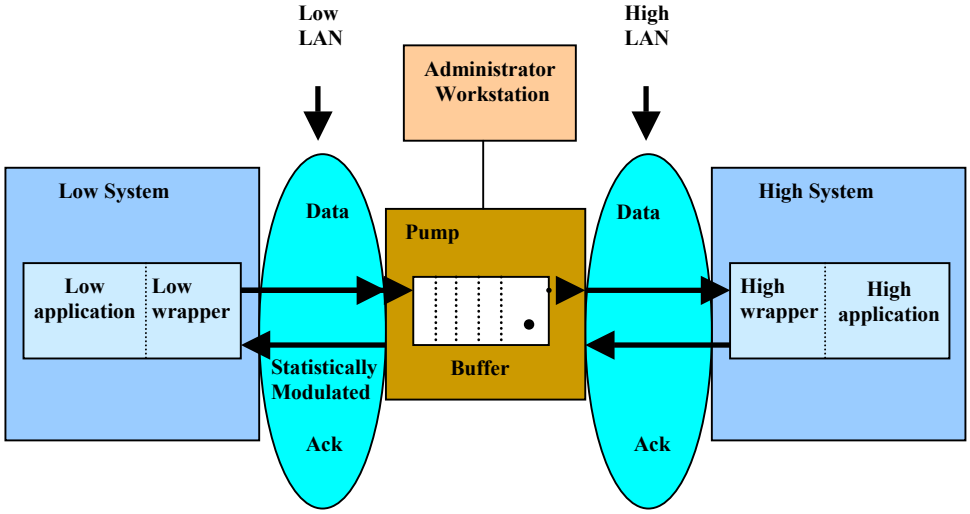

Figure 11. Architecture Overview
[Ref. 1]

1.3 Functional Description

1.3.1 System Capabilities

a. Support TCP/IP
   i. Implemented at application layer
   ii. Uses transport layer
   iii. Only operates with asynchronous applications

b. Use Wrappers
   i. Support Pump Protocol
   ii. Application portion/NP dependent part
   iii. Low Wrappers
      1. Request connection
      2. Send Data
      3. Close connection
   iv. High Wrapper
      1. Receive connection
      2. Review Message
      3. Send Acknowledgement
   v. Administrator Terminal (NP Console)
      1. Initial Configuration – define which users of Low LAN can open connections to which users on high.
      2. Changes in configuration
      3. Control Information
      4. User/performance reports (logging)
   vi. NP
      1. Reliable information transfer from Low to High while high information is not leaked to Low LAN.

2. Ensure LAN communications interface conforms to NP Protocol operating policy
3. Control timing of Ack sent across Low LAN interface to prevent covert channels from high to low
4. Store Data message in buffers
5. Establish High connections
6. Control Low LAN to High LAN connections; Re-establish if required.
7. Maintain configuration table
    a. Windows like interface
    b. Buffer size
    c. Time out period
    d. Port connections/host
    e. Port connections/NP
    f. IP address and port numbers for Low LAN
    g. IP address and port numbers for High LAN
8. Monitor error logging data structure – (list from security target)
9. Checklists
    a. Throughput
    b. Availability
    c. Accuracy/Validity
    d. Usage and Acknowledgement of Design
    e. Non-duplication
    f. Connection Independence
    g. Connection Fairness

1.3.2 System Criticality

The NP is a tool that increases the efficiency and the effectiveness of personnel onboard US Naval vessels. For this SSAA the NP is situated in an operational environment such that the loss of the NP could be absorbed for a period of days without having an adverse impact upon mission accomplishment. After more than two days without NP operation, the effectiveness of the unit degrades due to the additional labor required to accomplish the mission.

1.3.3 Classification and Sensitivity of Data Processed

Information stored, processed, and transmitted through the NP includes data from a low-security level system to a high-security level system. The degree of sensitivity (high, medium, and low) is used to identify specific information security requirements and cost effective measures to protect NP transferred information. All classified data are protected by measures appropriate for system high operations in accordance with DoD security requirements as specified in DoD Dir. 8500.1. Need-to-know controls are an element of protective measures placed on compartmentalized environments. In this SSAA we assume that the highest data processed will be Top Secret, Compartmentalized (One Classification and Multi-categories), the data types involved include Privacy act, financial, mission critical operation, proprietary, and administrative.

1.3.4 System User Description and Clearance Levels

The system users could include military, government, civilian, and contractor personnel. Users on the high side will be required to have, at a minimum, a security clearance equal to the security level of system receiving the data. All high side users must be cleared in accordance with local command's security requirements mandated for access to physical locations where the high side operates.

1.3.5 Life Cycle of the System

The NP is in a developmental state and is evolving from a single workstation with one server to multiple workstations using multiple servers. Once incorporated for use the compatibilities of the NP will be expand and future uses will be defined.

The NP is currently in the preliminary test and evaluation stages at NRL. The component is under continued development; the goal is that Test and Evaluation will be conducted by the end of FY03. Upon acceptance by DoD and DoN the system will be placed under configuration control of SPAWAR. Maintenance of the NP will be initially provided by NRL and SPAWAR until the completion of training of qualified military technicians. The maintenance concept for on-site repair will be isolation and replacement of faulty components. Faulty components will be transferred to a control facility for repair or replacement. On-site maintenance personnel will require a minimum of the DoD Top Secret level. Before being released from government control and custody, all defective system components containing non-volatile memory will be sanitized using DoD and command approved sanitation methods for Top Secret equipment.

1.4 System CONOPS Summary

The NP concept of operations is to provide a trusted, reliable interface for automating the transfer of data from low to high-level systems. This will allow the sharing of tactical information, and performance of analysis and administrative activities. Access to information from the Low LAN will be available almost immediately. This increased access to information will help support the activity in its mission.

2.0 ENVIRONMENT DESCRIPTION

2.1 Operating Environment

NP protection mechanisms include physical as well as environmental controls described in 2.1.1 and 2.1.2. The NP will operate in the high environment of an incorporated system. It will be located in a High environment to provide the appropriate physical security for the high-level data being processed by the NP. All administrative access to the NP will be by personnel in the secure physical high environment. There is no access to the NP from outside the high environment.

2.1.1 Facility Description

The NP facility requirement will require the facility requirements dictated by other high systems on the ship.

2.1.2 Physical Security

The same physical security required for the high side will be required to provide physical security for the NP.

2.1.3 Administrative

Only system administrators will have access to the administrator terminal (NP Console). Only system administrators will be authorized to perform maintenance on the NP to ensure that system administrator settings are not disrupted or removed. Each administrator will have their own login and password to ensure audit logs reflect system administrator usage and tasks performed. Administrator clearances must be at the highest level for systems receiving the data.

2.1.4 Personnel

A minimum of one system administrator (two is desired) trained in the maintenance of the NP will be required to conduct all NP maintenance.

2.1.5 COMSEC

COMSEC will obtain the system high requirements [that the NP is incorporated.]

2.1.6 TEMPEST

TEMPEST will obtain the system high requirements [that the NP is incorporated.]

2.1.7 Maintenance Procedures

System administrators with clearance, equal to that required for the high side physical environment, will conduct all NP maintenance. The technicians will be properly trained to troubleshoot and repair the NP to ensure the NP maintains the highest level of assurance.

2.1.8 Training Plans

All unit system administrators will undergo NP training prior to receiving and installing the NP in a classified system. Previously trained system administrators can provide On-The-Job training (OJT) to provide system administrator continuity in job turn over and ability to maintain network availability.

2.2 Software Development and Maintenance Environment

The NP is being developed in a Closed Security Environment.

2.3 Threat Description

The NP is subject to a range of generic threats applicable to most government information systems processing unclassified and classified information. A potential threat exists to the confidentiality, availability, and integrity of the information processed, stored, and transmitted by the system. A potential threat also exists to the availability of the assets of the Low LAN system to assist in executing the desired command mission. The potential threats to the NP are from natural and manmade sources. Natural disasters and damage can result from fire, water, wind, and electrical sources. Manmade threats are from those who would target the command LAN for espionage, criminal activity, unlawful use, denial of service, or malicious harm. External or internal agents of threat include espionage, terrorist, hackers, and vandals.

Insider threat: We believe the greatest threat to the NP is insider threat from a trusted agent who has access to the system. The most likely incident involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the system, one of its components, or information processed, stored, or transmitted by the system. The next most likely incident involves an authorized user who takes deliberate action to damage the system, one of its components, or its data for personal gain or vengeful reasons. Such a person could also engage in espionage, other criminal activity, or exploitation or expropriation of the assets of the system for personal gain. The NP will undergo covert channel analysis to mitigate potential risk from possible malicious attack.

These insider threats can be manifested in the following ways:

- The unauthorized reading, copying or disclosure of sensitive information.
- The execution of denial of services attacks.
- The introduction into the system of viruses, worms or other malicious software.
- The destruction or corruption of data (intentional or unintentional).

The most serious of all types of possible attacks against the system could be mounted by corrupted system administration personnel with their ability to alter or bypass most, if not all, of the system's protection mechanisms.

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

3.1 Hardware

NP and System Administrator terminal (NP Console).

3.2 Software

The software is a complex integration of the pump protocol and run time system services. In this environment, the NP operator/programmer is presented with standard interfaces that provide access to NP functionality, utilities, and management services. It is government development specialized software designed exclusively for the NP by NRL. The components are:

- Operating System
- Pump Protocol
- Access Control

The NP protocol utilizes a combination of personnel, physical and system security mechanisms to control access to the NP. To control initial system access, the NP Console utilizes a combination of user identification and an authentication (password) known only to that user. To control access to specific information and access to components of the NP, a set of system defined resource access control lists are used (such as discretionary access control (DAC) tables). The NP Console Security Policy provides the foundation for the system administration and operation of the NP security software and implementations.

Applications are accessed based upon user access privileges (sometimes termed profiles). At log on, system level software determines which applications, databases, levels of data (if mandatory access controls (MAC) is in effect), and executables an individual is allowed to access and execute. Applications resident on the NP Console are administrative applications.

3.3 Firmware

Not Applicable

3.4 System Interfaces and External Connections

NP Console – System Interface

The NP has a console interface. A VT100 compatible terminal or terminal emulator must be connected to this interface. The NP administrator uses the console to manage the NP.

NP

There are two standard Ethernet RJ-45 network interfaces (for High and Low interfaces). The console interface is a DB 9 connector. The high and low side need to be marked in accordance with COMSEC requirements. The NP has a built-in Uninterruptible Power Supply (UPS).

3.5 Accreditation Boundary

The physical scope and context of the assumed ship's LAN boundaries are up to the ship's premise routers (CISCO 4000 or others). The CISCO 4000 provides the ship its primary connection to the NOC via the Super High Frequency (SHF) system during underway periods. During in-port periods the ship connects to the pier side firewall. (The Low Wrappers and High wrappers reside with the respective Low LAN server and High LAN server.) Different layers belong elsewhere.

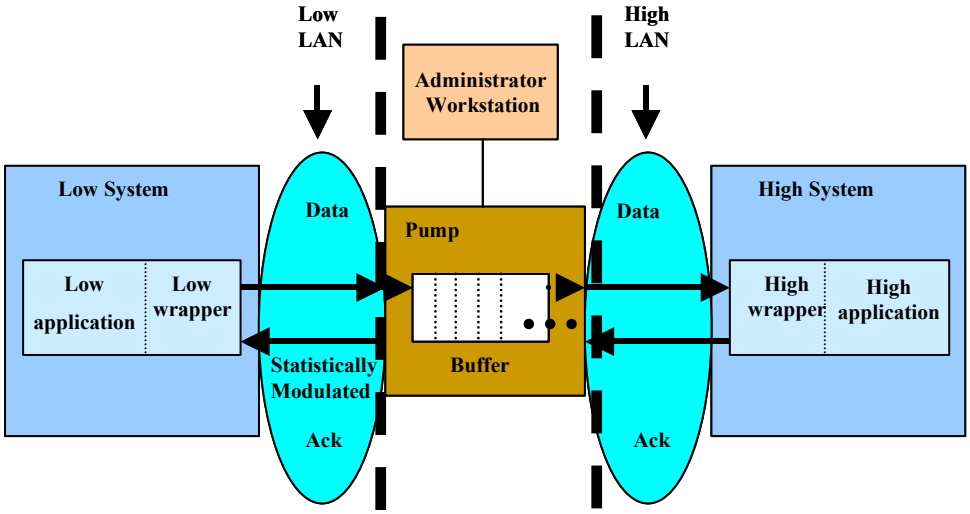

Figure 12. Type Accreditation Boundary
[Ref. 1]

4.0 ITSEC SYSTEM CLASS

In this section we describe the specific ITSEC modes that will apply to the NRL NP. We describe the specific alternative for each mode. The goal is to determine a total "weight" that can be used to determine the certification level.

4.1 Interfacing Mode

Active – An active system has direct interaction with other systems. With both physical and logical relationships the active case may allow multiple interactive sessions with multiple operations, systems, infrastructure, or data.

4.2 Processing Mode

Multi-level – In multi-level mode some of the users have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts but do not have a valid security clearance for all the information processed in the information system. All users have the proper security clearance, formal access approval, and a valid need-to-know for that information to which they have access.

4.3 Attribution Mode

Comprehensive – Comprehensive means all or almost all processing, transmission, storage, or data carries the need to attribute them to users or processes.

4.4 Mission-reliance factor

Cursory – Cursory means that the mission is only indirectly dependent on the specific aspect (the operation, data, infrastructure, or system).

4.5 Availability Factor

Reasonable – Reasonable means that the specific aspect (the operation, data, infrastructure, or system) must be available in reasonable time to avoid operational impacts.

4.6 Integrity Factor

Exact – Exact means that the degree of integrity for a specific aspect (the operation, data, infrastructure, or system) must be exact in order to avoid operational impacts.

4.7 Information Categories

Compartment/Special Access Classified – This category includes all information that requires special access and a security clearance. Examples include Sensitive Compartmented Information (SCI), Single Integrated Operations Plan – Extremely Sensitive Information (SIOP-ESI) and special access programs.

4.8 System Class Level

The certification team has determined the DITSCAP certification level to be Level 3.

Level 3 requires the completion of the minimum-security checklist and a more in depth, independent analysis.

4.9 Certification Analysis Level

Detailed Analysis

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w=0), Passive (w=2), **Active (w=6)**	6
Processing Mode	Dedicated (w=1), System High (w=2), Compartmented (w=5), **Multi-level (w=8)**	8
Attribution Mode	None (w=0), Rudimentary (w=1), Selected (w=3), **Comprehensive (w=6)**	6
Mission-Reliance Factor	None (w=0), **Cursory (w=1),** Partial (w=3), Total (w=7)	1
Availability Factor	**Reasonable (w=1),** Soon (w=2), ASAP (w=4), Immediate (w=7)	1
Integrity Factor	Not-applicable (w=0), Approximate (w=3), **Exact (w=6)**	6
Information Categories	Unclassified (w=1), Sensitive (w=2), Confidential (w= 3), Secret (w=5), Top Secret (w=6), **Compartmented/ Special Access Classified (w=8)**	8
	Total of all Weights	**36**

Table 23. Characteristics and Weights

Certification Level	Weight
Level l	If the total of the weighing factors in Table 23 is < 16.
Level 2	If the total of the weighing factors in Table 23 is 12 - 32.
Level 3	**If the total of the weighing factors in Table 23 is 24 - 44.**
Level 4	If the total of the weighing factors in Table 23 is 38 - 50.

Table 24. Certification Level

5.0 SYSTEM SECURITY REQUIREMENTS

5.1 National/DOD Security Requirements

The NP shall comply with requirements specified in ISO 15408. Design and implementation shall meet or exceed those contained under EAL5, Structured Protection. Federal Information Processing Standards (FIPS) publications, Office of Management and Budget circulars and bulletins, Executive Orders, and US legislative documents validate requirements articulated in DoD 8500.1. Additionally, the NP shall comply with those requirements necessary to implement requirements associated with ensuring compliance with the Privacy Act of the United States, Code 552a. The National, DoD, and DoN information assurance requirements are derived from the directives and instructions provided in the references.

5.2 Governing Security Requirements

The assumed security requirements for analysis and evaluation are provided in the Information System Security Policy (ISSP), Appendix D. The objectives stated in the ISSP were drawn from National, DoD, and DoN directives and instructions documented in the references. These references provide the governing security requirements.

5.3 Data Security Requirements

Many of the data security requirements depend on the security policy associated with the various categories and classifications of information processed on the system. Systems processing sensitive information also have additional security requirements. Table 25 identifies the types of data processed by the NP.

Data Type	Definition	System Applicability
	Non Sensitive Information	
	This category of information includes all information that is not classified and is not sensitive as defined below. Small programs, easily reconstructed. No effect on agency operations if data is lost or compromised. No financial liability	
	Sensitive Information	
Financial Sensitive	This category includes financially and contractually sensitive information. Information may be either classified or unclassified. Financially sensitive category information usually requires handling according to a common sensitivity, but may require special assurance mechanisms such as two-person verification of transactions. Financially sensitive category information requires system and information access control.	
Privacy Act	This category includes all information covered by the Privacy Act, including medical, pay, and personnel information. Information may be either classified or unclassified. Privacy Act category information requires handling according to a common sensitivity. Privacy Act information usually requires system and information access control.	
Administrative/ Other	This category includes DoD information associated with housekeeping activities, information marked For Official Use Only, sensitive company and customer information, and unclassified information that does not fall into any of the other information categories.	
Proprietary	This category includes information provided by a source or sources under the condition that it not be released to other sources. This information may require system or information access control.	
	Classified Information	
Confidential	Includes all classified information designated Confidential. The disclosure of confidential information could reasonably be expected to cause damage to national security. A security clearance is required for access to Confidential materials and systems.	

Data Type	Definition	System Applicability
Secret	Includes all classified information designated Secret. The disclosure of secret information could reasonably be expected to cause serious damage to national security. A security clearance is required for access to Secret materials and systems.	Yes
Top Secret	Category includes all classified information designated Top Secret. The disclosure of top-secret information could reasonably be expected to cause exceptionally grave damage to national security. A security clearance is required for access to Top Secret materials and systems.	Yes
Compartmented/ Special Access Classified	Category includes all information that requires special access and a security clearance. Examples include Sensitive Compartmented Information (SCI), Single Integrated Operations Plan-Extremely Sensitive Information (SIOP-ESI), and special access programs.	Yes

Table 25. Data Types

5.4 Security CONOPS

The NP security policy is enforced by the implementation, to the fullest extent possible, of EAL5. This includes controlling access to systems processing sensitive information by using identification and authentication mechanisms (e.g., passwords), and using protection features such as mandatory access controls, individual accountability and auditing.

5.5 Security Policy

Security Policy will be in accordance with all DoD security policies and local instructions.

5.6 Network Connection Rules

The connection of the NP to another network must be approved by the command Configuration Management process. Specific agreements regarding the resources required for the installation, operation, and maintenance of the security protection should be delineated in a Memorandum of Agreement between the appropriate officials responsible for the two network entities. The NP Memorandum of Agreement must be generated and owned by the DAA of the High side owner. Issues that pertain to rules related to the connection of the NP to other systems will consider the following:

- Sensitivity of the data processed on the network entities.
- Security characteristics of the interface device(s) between the two networks,
- Interface between the Computer Security Program Manager and the Computer System Security Officers (CSSO) for the two networks, respectively.

5.7 Configuration and Change Management Requirements

The NPs technical evaluation and type certification requires configuration management and control of hardware and software. Life-cycle configuration and change control shall be maintained over all NP hardware and software. Proposed changes to the NP software or hardware configuration will be reported to the program manager at SPAWAR PM-161 for a determination about the security implications of the change.

Configuration Management is enforced to assist in the overall security posture of the fleet.

5.8 Reaccredidation Requirements

OMB A-130 Appendix III requires the review of security documentation for each AIS when significant modifications are made to the federation/system or at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the federation/system. This periodic review includes a review of the AIS Security Plan, and a re-certification and re-accreditation process if required. The activities performed during the review and re-accreditation process are similar to those required during the initial C&A, except that areas where no change has occurred need only be verified that no change has occurred and that there is no impact to existing software/functionality by the introduction of the new capability/hardware/software. It does not require that the entire C&A process/test be redone. However, as a minimum, security documentation shall be reviewed and revised as appropriate under the following circumstances:

- Significant changes in the hardware, software, or data communications configuration.
- Changes in the security mode of operation.
- A breach of security, violation of system integrity, or unusual situation that appears to invalidate the certification.
- Three years have elapsed since the date of certification.

6.0 ORGANIZATIONS AND RESOURCES

6.1 Organizations

The organization comprises NRL as the NP developer, SPAWAR code 161 as the DDAA and Certifying Authority, and user representatives designated by the PM to provide fleet level experience and knowledge.

SPAWAR and user representatives are responsible for outlining the requirements associated with integrating the NP into operational systems. NRL is responsible for development and documentation of the NP to the Mission needs Statement of the user. SPAWAR is responsible for evaluation of the NP documentation and security aspects required for type certification and accreditation in accordance with the DITSCAP.

6.2 Resources

Type Certification

SPAWAR	-PM
SPAWAR	-DDAA
NRL	-Technical Expert and Certification Lead/Planners
User Rep	-Fleet Representative

Site Certification

CO	-DAA
SPAWAR	-Certification Authority
ISSM	-Certification Lead
User Rep	-Command System Administrator

6.3 Certification of Program of Record (POR) Components

Certification of the NP is the responsibility of NRL. Certification of the POR is the responsibility of the program manager's office. The program manager's office will provide the required system security documentation (SSAA, CT&E, SFUG, etc.) for the POR when delivered to the command.

6.4 Training

The site certification and accreditation teams require training on NP operations. The team shall have access to NP operator and maintenance manuals developed for fielding of the NP.

7.0 DITSCAP PLAN

7.1 Tailoring factors

The following subparagraphs identify DITSCAP tailoring factors that are designed to address the specific needs of the system, security requirements, and program requirements.

7.1.1 Programmatic Considerations

The hardware and software components of the defined system are identified in Section 3. There are plans to change, upgrade, or add to the current hardware or software components. Only one unique software application has been developed to integrate the various component software elements of the NP.

7.1.2 Security Environment

The security environment has been described in Section 5 with the ITSEC classification determination in Section 4. In determining certification level there are three characteristics that could affect the level of effort required. The processing mode could be changed if the environment falls under the compartmented definition. Integrity could significantly affect the level of effort if the threat to mission success, due to integrity, is determined to be very low causing this value to decrease. Finally, if mission reliance is determined to be none then the weight would also change.

7.1.3 IT System Characteristics

Since the software used in the NP is experimental, specialized code, incorporated into an experimental hardware device, the level of effort to certify and accredit the system may be significantly more than expected in the initial drafting of the SSAA.

7.2 Tasks and Milestones

The certification and accreditation team lead must develop a plan that contains tasks and milestones required to conduct security testing of the NP and culminating in awarding of an accreditation for the NP. The plan should contain the certification and accreditation schedule with estimated duration of individual tasks, team that are responsible for the activity, and completion criteria for each security-related function.

7.3 Schedule Summary

The DITSCAP schedule summary is all-inclusive.

7.4 Roles and Responsibilities

This section of the SSAA identifies the security related duties and responsibilities for each of the organizational and functional offices associated with the implementation and life cycle support of the NP. The system lifecycle is divided into four DITSCAP phases.

a. DITSCAP Phase 1, Definition. The Definition Phase includes activities to verify the system mission, environment and architecture, identify the threat, define the levels of effort, identify the Design Designated Approving Authority (DDAA) and Certification Authority (Certifier), and document the C&A security requirements. Phase 1 culminates with a documented agreement between the Program Manager, DDAA, Certifier, and user representative on the approach and results of the Phase 1 activities.

b. DITSCAP Phase 2, Verification. The Verification Phase includes activities to document compliance of the system with previously agreed on security requirements. For each life-cycle development activity, a corresponding set of security activities verifies compliance with the security requirements and constraints and evaluates vulnerabilities.

c. DITSCAP Phase 3, Validation. The Validation Phase includes activities to assure the fully integrated system in its specific operating environment and configuration provides an acceptable level of residual risk. Validation culminates in an approval to operate.

d. DITSCAP Phase 4, Post Accreditation. The Post Accreditation Phase includes activities to monitor system management, configuration, and changes to the operational and threat environment to ensure an acceptable level of residual risk is preserved. Security management, configuration management, and periodic compliance validation reviews are conducted. Changes to the system environment or operations may warrant beginning a new DITSCAP cycle.

7.4.1 Security Team Responsibilities

7.4.1.1 Design and Site Designated Approving Authority Responsibilities.

The DDAA and DAA must continuously review the system for compliance with the SSAA. During the C&A, the Certifier, and certification team support the DDAA/DAA. At other times, the DDAA/DAA is supported by the system ISSM. The DDAA/DAA's responsibilities during each of the DITSCAP phases are identified in Table 26 that is derived from rules and responsibilities outlined in DoD 8510.1-M [Ref. 2] chapters 3, 4, 5, and 6 for the DDAA/DAA.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
Define accreditation requirements.	Reviews SSAA to ensure it accurately describes the system, the threat, environment, security requirements, system vulnerabilities, and all conditions under which the system will be	Assess the vulnerabilities and residual risk.	Review proposed security changes.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
	operated.		
Obtain a threat assessment for the system.	Grant Interim Approval to Operate (IATO) if appropriate.	Decide if the security safeguards and residual risk are acceptable.	Oversee compliance validation.
Assign a Certifier to conduct vulnerability and risk assessments.		Approve/disapprove proposed corrective actions and countermeasures.	Monitor C&A integrity.
Support the DITSCAP tailoring and level of effort determination.		Determine if system should be granted full accreditation, interim accreditation, or an IATO.	Establish reaccredidation requirements and ensuring all assigned systems comply with these requirements.
Approve the SSAA.			Decide to reaccredit, or if the SSAA is no longer valid, terminate system operations.

Table 26. DDAA/DAA Responsibilities
[Ref. 2]

7.4.1.2 Certifier and Certification Team Responsibilities.

The Certifier and Certification Team responsibilities during each of the DITSCAP phases are identified in Table 27 that is derived from rules and responsibilities outlined in DoD 8510.1-M [Ref. 2] chapters 3, 4, 5, and 6 for the certifier.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
Support the DAA as the technical expert in the certification process.	Conduct the DITSCAP Phase 2 certification analysis tasks.	Complete the DITSCAP Phase 3 certification analysis tasks.	The Certifier and certification team normally are not involved with the system in Phase 4.
Begin vulnerability and risk assessments.	Identify and assess system vulnerabilities.	Maintain C&A schedules, plan of action and milestones based on performance of the technical effort.	
Review threat definition.	Report certification results to the DAA, program manager, and user representative.	Integrate changes to the security architecture and system security requirements into the SSAA.	
Identify the security requirements.	Provide advice to the DAA, program manager, and user representative regarding the readiness of the system to move into the	Identify and assess system vulnerabilities.	

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
	Validation Phase.		
Tailor the DITSCAP, determine the appropriate certification level, and prepare the DITSCAP Plan.	Maintain C&A schedules, plan of action, and milestones based on performance of the technical effort.	Recommend risk mitigation measures.	
Provide level of effort and resource requirements.	Integrate changes into the SSAA.	Report certification results to the DAA, program manager, and user representative.	
Develop the SSAA.		Prepare final SSAA (including all certification evidence).	
Provide oversight for the Certification Requirements Review (CRR).		Provide a recommendation for or against accreditation.	

Table 27. Certifier and Certification Team Responsibilities
[Ref. 2]

7.4.1.3 Information System Security Manager Responsibilities

During Phase 1 and 2 the ISSM is a member of SPAWAR. The ISSM supports the type certification team by performing the functions identified in Table 28. Once the NP is type certified, the ISSM becomes the security focal point within the local command, responsible for the secure operation of the system within the environment agreed upon in the SSAA. The ISSM ensures the system is deployed and operated according to the SSAA through integration of all the technical and non-technical security disciplines (COMPUSEC, COMSEC, EMSEC, personnel, Physical, and administrative procedures) to maintain an acceptable level of residual risk. The ISSM responsibilities during each of the DITSCAP phases are identified in Table 28 that is derived from rules and responsibilities outlined in DoD 8510.1-M [Ref. 2] chapters 3, 4, 5, and 6 for the ISSM.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
Assist the DAA, Certifier, and certification team in the certification effort.	Review the mission statement to determine if it accurately describes the system.	Serve as a member of the validation/certification team.	Periodically review the mission statement, operating environment, and security architecture to determine compliance with the approved SSAA.
Review the business case or mission statement to determine that it accurately describes the system.	Review the environment description to determine if it accurately describes the system.		Maintain the integrity of the site environment and accredited security posture.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
Review the environment description to verify that it accurately describes the system.			Ensure that configuration management adheres to the security policy and security requirements.
			Initiate the C&A process when periodic reaccredidation is required or system change dictates.
Initiate the dialogue with the DAA, Certifier, and user representative.	Develop system or system modifications.	Support certification team performance of Phase 3 tasks.	Report security related changes in the IS to the DAA and user representative.
Define the system schedule and budget.	Support the certification efforts by providing updates on the mission statement, environmental description, and architectural changes.	Provide access to the IS for the ST&E.	Update the IS to address reported vulnerabilities and patches under configuration management.
Support the DITSCAP tailoring and determine the certification level.	Review the certification results.	Approve system modifications as necessary to reduce or eliminate system vulnerabilities.	Review and update life-cycle management policies and standards.
Define the system architecture.	Approve system modifications as necessary to reduce or eliminate system vulnerabilities.		Resolve security discrepancies.
Integrate system security requirements into the system.			
Prepare Life-Cycle Management Plans.			
Define the security architecture.			
Determinate the level of effort.	Determinate the level of effort.	Determine the level of effort.	Determine the level of effort for recertification and reaccreditation's.
Support cost and schedule determinations.	Support cost and schedule determinations.	Support the cost and schedule determinations.	Support cost and schedule determinations for recertification and reaccredidation.
	Monitor progress.	Monitor C&A progress.	Maintain system documentation.
	Maintain system documentation.	Maintain system documentation.	
Provide technical equipment environment requirements.	Provide hardware and software architecture to the acquisition organization.	Develop or integrate technical security solutions and security requirements.	Provide hardware and software architecture to the acquisition organization.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
Provide target hardware and software architecture.	Provide technical equipment environment requirements to the acquisition organization.		Provide system modifications or changes to the ISSO and informing the program manager, DAA, Certifier, and user representative.
Provide information regarding the system development organization.	Develop or integrate technical security solutions and security requirements.		Develop or integrate technical security solutions and security requirements.
Determine the feasibility of technical solutions and security requirements.			

Table 28. ISSO Responsibilities
[Ref. 2]

7.4.1.4 User Representative Responsibilities

The user representative provides input into the SSAA to ensure that the system meets the operational need, will meet availability and integrity requirements, and has a realistic security policy that can be maintained in the operational environment. The User Representative responsibilities during each of the DITSCAP phases are identified in Table 29 that is derived from rules and responsibilities outlined in DoD 8510.1-M [Ref. 2] chapters 3, 4, 5, and 6 for the user representative.

DITSCAP Phase 1 Definition	DITSCAP Phase 2 Verification	DITSCAP Phase 3 Validation	DITSCAP Phase 4 Post Accreditation
Support the DITSCAP tailoring and level of effort determination.	Support certification actions.	Support certification actions.	Oversee the system operation according to the SSAA.
Provide a business case or mission statement.	Prepare Security Rules of Behavior and Standard Operating Procedures.	Implement and maintain Standard Operating Procedures and Rules of Behavior.	Report vulnerability and security incidents.
Validate or define system performance, availability, and functionality requirements.	Provide changes to the mission statement, functional environment, and organizational structure to the certification team.	Provide changes to the mission statement, functional environment, and organizational structure to the certification team.	Report threats to the mission environment.
Provide data sensitivity, end user functionality, and user organization information.	Verify the feasibility of security solutions and the ability to comply in the operational environment.	Review certification results.	Review and update the system vulnerabilities.
Verify the ability to comply with the SSAA during operations.			Review changes to the security policy and standards.
			Initiate SSAA review if there are changes in the threat or system configuration.

Table 29. User Representative Responsibilities
[Ref. 2]

7.4.2 Acquisition or Maintenance Organization Responsibilities

7.4.2.1 Configuration Management Responsibilities

The configuration management duties are integrated into the ISSM responsibilities.

7.4.2.2 System Administration Responsibilities

The System Administrator responsibilities include:

- Assist the validation/certification team in testing the system.
- Operate the system according to the SSAA.
- Maintain an acceptable level of residual risk.
- Inform the ISSO of any proposed changes or modifications to the system, information processed, operating procedures, operating environment that affect security.

ACRONYM LIST

ACC	Agency Computer Center
AIS	Automated Information System
C&A	Certification & Accreditation
CONUS	Continental United States
CSSO	Computer Systems Security Officer
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DISA	Defense Information System Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
E-Mail	Electronic Mail
FIPS	Federal Information Processing Standard
INFOSEC	Information System Security
ISSO	Information Systems Security Officer
LAN	Local Area Network
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI 4009	National Security Telecommunications and Information Systems Security Instruction Glossary
OMB	Office of Management and Budget
PM	Program Manager
POC	Point of Contact
RTM	Requirements Traceability Matrix
SAV	Security Assessment Visit
SBU	Sensitive But Unclassified
SSAA	System Security Authorization Agreement
ST&E	Security Test and Evaluation
TCSEC	Trusted Computer Security Evaluation Criteria
TCP/IP	Transmission Control Protocol/Internet Protocol
USERID	User Identification

WAN	Wide Area Network
WWW	Worldwide Web

REFERENCES

[1] Kang, Myong H. (1998). *Design and Assurance Strategy for the NRL Pump*. Retrieved April 18, 2002 from, http://chacs.nrl.navy.mil/publication/chacs/1998/1998kang-IEEE.pdf.

[2] DoD 8510.1-M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, July 31, 2000.

[3] 28 CFR Part 17 - National Security Information Program.

[4] 5 CFR Part 930.

[5] Director of Central Intelligence Directive (DCID) 1/16.

[6] DoD 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997.

[7] Executive Order 12356, National Security Information.

[8] ISO 15408 Version 2.1, Common Criteria for Information Technology Security Evaluation, August 1999.

[9] NACSIM 7000 TEMPEST.

[10] National Security Agency (NSA) Manual 90-2, "COMSEC Material Control Manual".

[11] NAVIA Pub 5239, Information Assurance Publication Series.

[12] OMB Bulletin 90-08, Individual Security Plan Guidance.

[13] OMB Circular A-123, Management Accountability and Control, June 21, 1995.

[14] OMB Circular A-130, Management of Federal Information Resources, Appendix III - Security of Federal Automated Information Resources, February 16, 1996.

[15] OPNAVINST 5230.24, Navy and Marine Corps Policy on the use of Compact Disc Technology, November 18, 1993.

[16] Privacy Act 5 United States Code 552a.

[17] Public Law 100-235, Computer Security Act of 1987, 8 January 1988.

[18] SECNAVINST 5239.3, DoN Information Systems Security Program, January 17, 1997.

[19] SECNAVINST 5510.30A, Department of the Navy Personnel Security Program, March 10,1999.

[20] SECNAVINST 5510.36, Department of the Navy Information Security Program (ISP) Regulation, March 17, 1999.

[21] SECNAVINST 5720.47, DoN Policy for Content of Publicly Accessible World Wide Web Sites, July 1, 1999.

[22] The Trusted Network Interpretation (TNI) of the TCSEC, National Computer Security Center Technical Guide 005 (NCSC-TG-005).

INFORMATION SYSTEMS SECURITY POLICY (ISSP)

1. The Designated Approving Authority (DAA) shall ensure continuous employment of appropriate physical, administrative and technical measures designed to protect the information system and its data, detect any penetration or compromise, and correct/restore any unauthorized modification or destruction of information and protect users against denial of service.

2. Claimant DAA's

a. The DAA for information systems processing National Crypto logic data is COMNAVSECGRU.

b. The DAA for information systems processing SCI information is COMNAVINTCOM.

c. The DAA for information systems processing SIOP-ESI is the Chief of Naval Operations (CNO).

d. The DAA for all other information systems processing Top Secret, Secret, Confidential or Sensitive Unclassified not previously identified is the Commanding Officer.

3. All information systems under the cognizance of a DAA other than the designated Commanding Officer shall conform to the conditions set forth by this security policy and the command DAA. The connection of systems not under the DAA authority shall have an approved MOA between the Commanding Officers of each activity.

4. All information systems under the purview of this plan shall meet the requirements outlined in DODINST 5200.40, DOD Information Technology Security Certification and Accreditation Guide. Exceptions require prior written approval of the command Information Systems Security Manager (ISSM).

5. Access to information systems, networks and other computer resources shall be controlled and monitored to ensure each person having access can be identified and held accountable for their actions. An information system, network or other computer

resource will follow the "least privilege" principle so that each user is granted access to only the information to which the user is entitled by virtue of security clearance and formal access approval and only the resources necessary to perform assigned functions. In the absence of a specific positive grant of access, user access defaults to "no access".

6. A specific security mode of operation (Dedicated, System High) shall be designated for each information system. Stand- alone microcomputers and LAN workstations processing sensitive unclassified/classified information shall operate in the DEDICATED mode of operation. All Local Area Networks processing up to SECRET information shall only operate in the System High mode of operation.

7. Encryption methods, standards and devices used to protect classified data processed by an information system; network or computer resource must be approved or validated by NSA.

8. All shipboard unclassified systems are determined to be sensitive but unclassified per SECNAVINST 5239.3.

9. Software shall be thoroughly tested and verified in a "stand-alone" or “test” environment. Additionally, the command ISSM prior to use must approve installation and use of the software.

10. Copyright laws shall be enforced to ensure no unauthorized software duplication occurs. The command ISSM will coordinate with command Information Systems Division/Departments and will be primarily responsible to ensure the command adheres to copyright laws.

11. The command ISSM will accreditate/re-accreditate command procured local area networks, LAN workstations, and laptops IAW DODINST 5200.40 DOD Information Technology Security Certification and Accreditation Guide.

12. The ship fully supports the requirements of the Controlled Access Program (CAP), and shall meet these mandates for all information systems (classified and sensitive unclassified). CAP controls to be provided by information systems personnel to ensure a fundamental level of protection are:

- Identification and Authentication
- Discretionary Access Control
- Audit capability
- Object Reuse

13. A Risk Management program shall be implemented to determine how much protection is required, how much exists and the most economical way of providing needed protection.

14. The ship will conduct a Risk Assessment and a Security Test and Evaluation (ST&E) on each information system or group of similar information systems using

DODINST 5200.40. This will be accomplished by the command Information Systems Security Manager (ISSM), Network Security Officer (NSO) and the command Information System Security Staff.

15. The command ISSM will ensure that the Contingency Plan for all command Information Systems are current and updated as required. Additionally, the Contingency Plan will be tested and documented for all mission critical information systems. This includes essential administrative support information systems. Emergency destruction shall be addressed in the Contingency Plan.

16. The accreditation statement shall specify constraints under which the system may operate, including the security modes of operation, external system interconnections, user authorization requirements, system configuration, and location.

17. All Information Systems Security documentation disclosing capabilities, vulnerabilities, or limitations shall be marked at a minimum, For Official Use Only (FOUO).

18. All Information System Security violations shall be reported immediately to the command Information Systems Security Manager (ISSM) for immediate action and resolution. The command ISSM is responsible in keeping the DAA informed of such incidents, as well as providing recommendations to resolve these incidents. Additionally, the command ISSM will provide the command Security Manager a copy of the incident report.

19. Prior to public disclosure or discussion of specific capabilities, limitations or vulnerabilities of information systems comply with Chapter 5 of SECNAVINST 5720.44A, Department of the Navy Public Affairs Policy and Regulations and OPNAVINST 5510.1H.

20. Configuration management for hardware and software will be maintained by the command Information Systems Department.

21. Any Information System operating temporarily outside this instruction shall adhere to requirements of this ISSP. In addition, users shall pay particular attention to information security requirements when processing or storing classified data.

22. The command ISSM will establish an Information System Security Awareness Training Program and include (as a minimum):

- Security notices, pamphlets or newsletters, when received, will be circulated via administrative channels.
- Annual GMT lectures and classroom training will be provided as well as Information Assurance Indoctrination briefs for all newly reporting personnel.
- Provide on-site training to activity Information Systems Security Staff on Risk Assessment, Security, Test & Evaluation, and Contingency Plan.

23. An Information System Security Policy (ISSP) shall be included in all information system support contracts, Memorandum of Understanding (MOU) and Communications Support Agreements (CSA).

24. When information systems under the jurisdiction of separate DAAs are interconnected, a Memorandum of Agreement (MOA) shall be established that states the minimum Information Assurance requirements to be satisfied by the individual systems and their interconnections. The MOA shall describe the interconnections between information systems and the allowed interactions; describe the data flow between the systems including classification and sensitivity of the data, specify user authorization requirements and specify safeguards that are required before the interconnections become operational. The MOA shall be signed by each DAA whose system is part of the interconnection. When the interconnection involves more than two information systems, a lead DAA shall be mutually agreed upon who will be responsible for resolving conflicts. This policy applies to the interconnection of DON information systems with other DON facilities, military departments, government agencies, and allied systems.

25. Privately Owned Resources

The use of privately owned or leased equipment (e.g., contractor) or information systems (e.g. microcomputers, public computer services, public telecommunications services) or software (e.g. system, applications) to support DoN functions or operating within DoN activities is prohibited without the prior written authorization of the Designated Approving Authority. All privately owned resources shall meet the requirements of this instruction. Classified data shall not be processed or transferred using privately owned resources.

26. Entertainment Software

Entertainment software such as music CD's can be used on ships Information Systems with CD-ROM drives or at Designated Approving Authority's discretion. All other entertainment software on U.S. Government resources is strictly prohibited unless the software directly supports the organization's mission. Entertainment software installed and/or used on a Government resource is subject to removal and disciplinary action taken against the violator.

27. Virus Protection

All file servers, LAN workstations, stand-alone PCs, and laptops will have an anti-virus program installed. Additionally, virus signature files will be updated and kept current to minimize virus infections to local area networks and AIS assets. The command ISSM, NSO and Information Systems personnel are responsible that the command anti-virus programs are updated and operational on all command AIS assets. When a virus is detected, users should notify the IS Help Desk.

The command ISSM will ensure timely submission of computer virus reports is submitted via naval message or by e-mail to NAVCIRT@FIWC.NAVY.MIL or NAVCIRT@FIWC.NAVY.SMIL.MIL with the following reporting format:

- NAME OF THE INFECTING VIRUS

- SOURCE AND DATE OF THE VIRUS, IF KNOWN
- OTHER LOCATIONS, WITHIN OR OUTSIDE OF YOUR COMMAND, POSSIBLY INFECTED AS A RESULT OF THIS VIRUS
- NUMBER AND TYPE OF SYSTEMS INFECTED
- METHOD OF CLEAN-UP
- NUMBER OF MAN-HOURS REQUIRED IN EFFORT
- DAMAGE OR OBSERVATIONS RESULTING FROM THE VIRUS TRIGGERING
- YOUR COMMAND AND LOCATION
- POINT OF CONTACT AT YOUR COMMAND

28. Information Conditions

Information Conditions were established in response to increased computer network attacks. INFOCONS are analogous to THREATCON levels. Events that would raise or lower those levels may directly affect the existing INFOCON level. Information Condition Levels are Normal **ALPHA** (Low Activity), **BRAVO** (Significant Activity), **CHARLIE** (Serious Activity), and **DELTA** (Critical Activity). Events that would raise or lower those levels may directly affect the existing INFOCON level. However, INFOCONS are independent from DEFCON and THREATCON levels. These response measures are directive and do not simply provide information security advisories. All claimant activities will adhere and enforce INFOCON Conditions when directed.

29. Reporting of Computer Network Incidents

All successful and unsuccessful computer network incidents will be reported. Reports on probes, successful/unsuccessful intrusions will be submitted within 2 hours of validation of the incident. Initial reports may not include all data, and may require follow-up reports. Reports may be sent via E-mail. Successful Computer Network Intrusions Reports for Sensitive But Unclassified (SBU) systems will be submitted via naval message or SIPRNET to: NAVCIRT@FIWC.NAVY.SMIL.MIL. Reports of unsuccessful Computer Network Intrusions and probes on SBU systems will be classified as UNCLASSIFIED FOUO and will be reported via naval message or NIPRNET E-mail when other means are not practical to: NAVCIRT@FIWC.NAVY.MIL. All successful computer network intrusions for SIPRNET and JWICS systems will be classified as SECRET. Unsuccessful computer network intrusions, probes, or port scans reporting will be classified as SECRET.

30. Network Pollution

Upon receipt of a classified attachment to UNCLAS E-Mail, users should take the following action:

- Immediately notify Information Systems Help Desk.
- The Help Desk will notify the Network Security Officer (NSO) and Information Systems Security Manager (ISSM). The ISSM will direct all corrective actions and provide report status of actions completed to the Commanding Officer via Executive Officer and Department Head.
- Upon finding a classified document on the UNCLAS LAN (or TS/SCI document on the SECRET LAN), users shall not delete or forward the

illegal document, or do any further processing until the Network Security Officer (NSO), Information Systems Security Manager, and/or Information Systems personnel arrive on the scene to declassify the workstation, and authorize the user to continue processing. Meanwhile, until the NSO, ISSM or IS personnel arrive on the scene; the workstation must be guarded by a person with the appropriate security clearance.

31. Internet/E-mail Policy

As our Sailors, Marines, and civilians become proficient in accessing the Internet, the following policy promotes the widest permissible use of government information systems to access and exchange information in an automated environment. This includes, but is certainly not limited to, accessing the Internet, browsing the World Wide Web, and communicating via Electronic Mail.

Consistent with the Legal and Security rules described below, fleet personnel, military and civilian, are encouraged to use their government computers to access the Internet and develop their information skills. To that end, we recognize that the best way to develop your Information Technology skills is to get on the Net and make it your preferred and routine choice to access, develop and exchange information.

DOD Directive 5500.7-R, JOINT ETHICS REGULATION, Section 2-301 supports this approach and recognizes that official uses of Information Systems include uses that previously may have been interpreted as personal uses. Consistent with DOD Directive 5500.7-R, this instruction makes the following finding: Any permissible use of the Internet enhances the users professional skills and thus serves a legitimate public interest.

Permissible uses are defined to include all uses not prohibited by Law, Regulation, Instruction, or Command Policy. Prohibited uses include:

- Introducing classified information into an unclassified system or environment.
- Accessing, storing, processing, displaying, distributing, transmitting or viewing material that is Pornographic, Racist, promotes of Hate Crimes, or subversive in nature.
- Storing, accessing, processing, or distributing Classified, Proprietary, Sensitive, For Official Use Only (FOUO) or Privacy Act protected information in violation of established security and information release policies.
- Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.
- Knowingly writing, coding, compiling, storing, transmitting or transferring malicious software code, to include viruses, logic bombs, worms and macro viruses.
- Promoting partisan political activity.
- Disseminating religious materials outside an established command religious program.

- Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property, with the exception of utilizing a command approved mechanism such as a Welfare and Recreation Electronic Bulletin Board for advertising personal items for sale.
- Fund raising activities, either for profit or non-profit unless the activity is specifically approved by the command (e.g. Welfare and Recreation Car Washes).
- Gambling, wagering or placing of any bets.
- Writing, forwarding or participating in chain letters.
- Posting personal home pages.

All users are reminded that they have no expectation of privacy in their use of Government Information Systems. Use of Government Information Systems, including use of the Internet and E-mail, is subject to monitoring, interception, accessing and recording, and may be passed to law enforcement. Any violation of the above policies can result in Disciplinary or Administrative action.

NCIS has an active Computer Crime and Counterintelligence Response Program with teams in each field office. Contact should be made whenever evidence is discovered that a Government Information System is being used for Criminal or Foreign Intelligence purposes.

Commanders and Commanding Officers have the authority to control or limit the use of Government Information Systems for the purposes of Security, Morale, Good Order and Discipline and to promote the efficiencies of their command. This authority may be delegated to System Administrators. For example, A Commander could authorize a System Administrator to block access to specific sites, limit Internet due to resource constraints or revoke an individual's Internet Access and use of Government Information System altogether. Similarly, a Commander could place limits on the size and type of electronic files that could be downloaded, so as to prevent the system from being overburdened.

32. Web page policy

Ships publicly accessible Web Pages will be registered with the Government Information Locator Service (GILS). Ships Web pages will have a .mil domain. Additionally, information on all ship Web pages will be official, approved and released by the Commanding Officer and/or Public Affairs Officer. Ships publicly accessible web pages will be subject to semi-annual on-line surveys conducted by Fleet Information Warfare Center (FIWC).

33. On-line Surveys

Ships local area networks (LANs) will be subject to un-announced on-line surveys by the FIWC on a semi-annual basis. The purpose for these surveys is to assess vulnerabilities of command LANs. Results of the on-line surveys will be made available to the command ISSM by FIWC for review and corrective actions as required. Questions, concerns or requests for specific on-line surveys for the ship can be forwarded to the command ISSM.

34. Firewall/Intrusion Detection

The ship is configured as a trusted host behind the NOC Firewalls. The fleet firewall policy will be used by regional NOCs. Ship is configured behind the pier side Firewall for Internet and SIPRNET connectivity. NIPRNET/SIPRNET Firewall waiver requests will be forwarded to the appropriate fleet Information Assurance Office via naval message for consideration.

35. Remote Access

Use of dial-up lines, other than those that are protected with nationally certified cryptographic devices or protected distribution systems (PDS), will not be allowed for gaining access to systems resources that process classified information, unless the DAA provides specific written authorization for a system to operate in this manner in rare and limited circumstances. Remote access requires the use of enhanced identification and authentication mechanisms to protect against eavesdropping on the communication links.

36. Communications Security (COMSEC)

The communications links connecting the components of network information systems, associated data communications, shall be protected in accordance with national policies and procedures applicable to sensitivity level of the data being transmitted.

37. DOD Warning Banners

All official automated information systems (AIS) will display the DoD legally approved logon-warning banner. The DoD Warning Banner also serves to provide notification of, and consent to, COMSEC monitoring.

38. Network Security Tools

Network Security Tools will only be used by the command ISSM, NSO and Information Systems personnel. Users other than those personnel identified will not procure or download such tools. Procurement of such tools will be approved by the command ISSM and can be downloaded from the Navy INFOSEC Homepage, obtained from SPAWAR PMW-161, or through open purchase. At no time will the command ISSM, NSO or Information Systems personnel use these tools on another command's AIS system without approval from the local DAA and the requesting activity DAA. Additionally, these tools are not to be used to scan public, private and/or commercial systems on the Internet. Any violation of this policy will result in Disciplinary or Administrative Action.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Brotzman, Robert L. (1985). *Computer Security Requirements: Guidance for Applying the TCSEC in Specific Environments*. Retrieved May 7, 2002, from http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-003-85.html.

[2] *Course Notes CS3600, Introduction to Computer Security*. NPS CISR, Naval Postgraduate School, Winter 2002.

[3] Kang, Myong H. (1998). *Design and Assurance Strategy for the NRL Pump*. Retrieved April 18, 2002 from, http://chacs.nrl.navy.mil/publication/chacs/1998/1998kang-IEEE.pdf

[4] Department of the Navy Information Management and Information Technology Strategic Plan for FY 2002-2003. *Retrieved June 1, 2002 from* http://www.don-imit.navy.mil/stratplan.html

[5] CNO/GENADMIN/091943Z JUN 00. Certification and Accreditation of Systems and Networks. Retrieved February 12, 2003, from http://infodec.navy.mil/pub/docs/documents/navyn/cnomssg/091943_jun_00.txt.

[6] Department of Defense Directive No. 8500.*1 Information Assurance*, October 24, 2002.

[7] National Computer Security Center. *Department of Defense TCSEC, (DoD 5200.28-STD) "Rainbow Series"*, January 1994. Retrieved May 5, 2002, from http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[8] *Common Criteria for Information Technology Security Evaluatio*n, CCIB-99-031 through 033, Parts 1,2 and 3, Version 2.1, August 1999.

[9] Department of Defense Instruction No. 5200.40. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). December 30 1997.

[10] OPNAV Instruction No. 5239.1B. Navy Information Assurance (IA) Program, November 9, 1999.

[11] National Computer Security Center. *Introduction to Certification and Accreditation, "Rainbow Series"*, January 1994. Retrieved April 21, 2002, from http://www.disa.navy.mil.

[12] National Computer Security Center. *Trusted Network Interpretation environments guideline, "Rainbow Series"*, January 1994. Retrieved May 7, 2002, from http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-011.html.

[13] Brotzman, Robert L. (1985). *Computer Security Requirements: Technical Rational Behind the Environment Guidelines*. Retrieved May 7, 2002, from http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-004-85.html.

[14] Naval Research Laboratory *Network Pump (NP) Security Target*, May 29, 2000. Retrieved Feb 12, 2003, from http://chacs.nrl.navy.mil/publications/CHACS/2000/2000moore-NPST.pdf

[15] CAPP, Retrieved February 12, 2003, from http://niap.nist.gov/cc-scheme/PP_LSPP_V1.b.html.

[16] LSPP, Retrieved February 12, 2003, from http://niap.nist.gov/cc-scheme/PP_LSPP_V1.b.html.

[17] *Defense of Defense Mail Guard for High Robustness Environments Protection Profil*e, Version 0.1, September 30, 2001.

[18] NIAP Website. Retrieved February 12, 2003 from http://niap.nist.gov/niap/index.html.

[19] John Mildner, Email Discussion. January 25, 2003.

[20] Department of the Navy Information Assurance Publication No. 5239-13 Vol II. Information Assurance Certification and Accreditation (C&A) Publication Volume II: Site, Installed Program of Record, and Locally Acquired Systems.

[21] Department of the Navy Information Assurance Publication No. 5239-13 Vol III. Information Assurance Certification and Accreditation (C&A) Publication Volume III: Program of Record Information Systems.

[22] *Digital Signature Standard (DS*S), FIPS PUB 186-2, January 2000.

[23] *Secure Hash Standar*d, FIPS Pub 180-1, April 1995.

[24] 2001 *Information Assurance Technical Framewor*k, Version 3.0, September 2000.

[25] Department of Defense Instructions, Serial number 8510.1 July 2000. *DOD Information Technology Security Certification and Accreditation Process (DITSCAP)*.

[26] Draft Department of Defense Instruction, *IA Implementation 8500.b*b, June 7, 2001.

[27] Department of Defense Directive No. 4630.5. Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), January 11, 2002.

[28] Department of Defense Directive No. 4630.8. Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 2, 2002.

[29] Department of Defense Directive No. 8000.1. Management of DoD Information Resources and Information Technology, February 27, 2002.

[30] Department of Defense Directive No. 5160.54. Critical Asset Assurance Program (CAPP), January 20, 1998.

[31] Secretary of the Navy Instruction No. 5510.36 CH-2, Department of the Navy (DON) Information Security Program (ISP) Regulation, January 23, 2001.

[32] Department of the Navy Information Assurance Publication No. 5239-01. Introduction to Information Assurance (IA) Publication.

[33] Department of the Navy Information Assurance Publication No. 5239-13 Vol I. Information Assurance Certification and Accreditation (C&A) Publication Volume I: Introduction to Certification and Accreditation.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. LCDR Raymond Buettner
   Naval Postgraduate School
   Monterey, California

4. Daniel C. Boger
   Naval Post Graduate School
   Monterey, California